

# GROUPES

Classification Thèmes de MegaMaths

Docs de Dany-Jack MERCIER

# Groupes opérant sur un ensemble. groupes de SYLOW

(Dany-Jack MERCIER, 1979)

[ugre-groupesdesylow.pdf]

Définition - Équation des classes.

On dit qu'un groupe  $G$  opère sur un ensemble  $E$ , à gauche, si  $\exists$  loi externe

$$\begin{aligned} G \times E &\longrightarrow E \\ (g, x) &\longmapsto g.x \end{aligned}$$

qui vérifie :

- 1)  $g.(g'.x) = (gg').x \quad \forall g, g' \in G \quad \forall x \in E$
- 2)  $e.x = x \quad \forall x \in E$

Th | L'ensemble  $E$  est un  $G$ -ensemble si et seulement si  $G$  est isomorphe au groupe  $S(E)$

NB :  $S(E)$  est le groupe symétrique de  $E$ , c.à.d. le groupe de toutes les permutations de  $E$  dans  $E$ , muni de  $\circ$ .  
d'homomorphisme  $T: G \rightarrow S(E)$  annoncé n'est autre que  $T_g(x) = g.x$ .

Définitions :

a)  $G$  opère fidèlement sur  $E$  si  $T: G \rightarrow S(E)$  est injectif, c.à.d. si  $gx = x \quad \forall x \in E \Rightarrow g = e$

b)  $Gx = \{ y \in E / \exists g \in G \quad y = g.x \} =$  orbite de  $x$  pour le groupe  $G$ .

c)  $H_x = \{ g \in G / gx = x \}$  est un sous-groupe de  $G$ . C'est le sous-groupe d'isotropie, ou "stabilisateur" de  $x$  dans  $G$ .

Th | Soit  $\Omega$  une orbite pour  $G$ . Si  $x$  et  $y$  sont éléments de  $\Omega$ , alors les groupes d'isotropie  $H_x$  et  $H_y$  sont conjugués dans  $G$ .

On remarque que la relation dans  $E$  :  $x \sim y \Leftrightarrow \exists g \in G \quad y = gx$  est une relation d'équivalence, et que les classes de  $\sim$  ne sont autres que les orbites dans  $E$  :

plus précisément :  $x_{(G)} = Gx$   
Les orbites de  $E$  forment donc une partition de  $E$ .  
Mentions le théorème :

$$x, y \in \Omega = Gx \Leftrightarrow \exists \sigma \in G \quad x = \sigma.y$$

Donc :

$$\begin{aligned} h \in H_x &\Leftrightarrow h.x = x \Leftrightarrow (h\sigma).y = \sigma.y \Leftrightarrow (\sigma^{-1}h\sigma).y = y \\ &\Leftrightarrow \sigma^{-1}h\sigma \in H_y \Leftrightarrow h \in \sigma H_y \sigma^{-1} \end{aligned}$$

d'où  $H_x = \sigma H_y \sigma^{-1}$ , ce qui signifie que le sous-groupe  $H_x$  est le conjugué de  $H_y$ .  
CQFD

$\beta_x$  se factorise canoniquement puisque :

$$\beta_x(g_1) = \beta_x(g_2) \Leftrightarrow g_1 \cdot x = g_2 \cdot x \Leftrightarrow g_2^{-1} g_1 \cdot x = x \Leftrightarrow g_2^{-1} g_1 \in H_x$$

Ainsi, le diagramme suivant est commutatif :

$$\begin{array}{ccc} G & \xrightarrow{\beta_x} & \beta_x(G) = G_x \\ \pi \downarrow & \nearrow \theta \text{ homomorphisme} & \\ G/H_x & & \end{array}$$

classes à gauche suivant le sous-groupe d'isotropie  $H_x$ .

Ainsi, si  $G$  est finie :  $\# G_x = \# G/H_x = \frac{\# G}{\# H_x}$

$$\boxed{\# G_x = \frac{\# G}{\# H_x}}$$

Equation des classes :

Si l'ensemble  $E$  est fini, chaque orbite est un ensemble fini. Si  $E' \subseteq E$ ,  $E'$  ne contient qu'un élément et un seul de chaque orbite, alors, en regardant la partition réalisée par la relation  $\sim$  dans  $E$  :

$$\boxed{\# E = \sum_{x \in E'} \# G_x = \sum_{x \in E'} \frac{\# G}{\# H_x}} \quad (\text{équation des classes})$$

Exemple :  $G$  groupe fini.  $\varphi : G \rightarrow \text{Int}(G) \subset S(G)$   
 $g \mapsto \varphi_g \quad / \quad \varphi_g(x) = g x g^{-1}$

$\varphi$  est un épimorphisme de groupes.

C'est donc un  $G$ -ensemble pour la loi dite de conjugaison :  $G \times G \rightarrow G$

$$H_x = \text{stabilisateur de } x = \{g \in G / g x = x g\}$$

Si  $z \in Z(G)$   $H_z = G$  et réciproquement. Donc  $\# G_z = 1$

L'équation des classes implique :  $\# G = \sum_{x \in Z(G)} \# G_x + \sum_{x \in A} \# G_x$

( $A$  = ensemble des éléments de  $G$  tel que 2 éléments quelconques de  $A$  ne sont pas conjugués). Ainsi :

$$\boxed{\# G = \# Z(G) + \sum_{x \in A} \# G_x}$$

exercice :  $p \in \mathbb{P}$ ,  $G$  groupe d'ordre  $p^k$ . Or  $Z(G)$  n'est pas trivial.  
 [Sol : Pour  $x \notin Z(G)$ ,  $\# G_x$  divise proprement  $p^k$  donc est une puissance de  $p$ .  
 On a  $\# Z(G) = \# G - \sum_{x \notin Z(G)} \# G_x \Rightarrow \# Z(G) \equiv 0 \pmod{p} \Rightarrow Z(G) \text{ non trivial}$  ]  
 (théorème de Burnside)

groupes primaires, groupes de Sylow 19/ Définitions et premières propriétés.

Th 1 | Tout groupe fini commutatif contient un élément d'ordre  $p \in \mathcal{P}$  si  $p \mid \#G$

Th 2 | Soit  $G$  un groupe fini d'ordre  $n$ , et  $p \in \mathcal{P} / p^k \mid n$ .  
Alors  $G$  contient un sous-groupe d'ordre  $p^k$

preuve: le théorème est trivial si  $n = p^k$ .  
On raisonne par récurrence sur  $n$  en supposant le théorème vrai pour tous les groupes d'ordre  $n' < n$ .

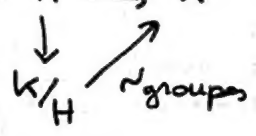
$G$  est un  $G$ -ensemble pour la loi de conjugaison  $(g, x) \mapsto gxg^{-1}$ .  
De 2 choses l'une:

a)  $\exists x \notin Z(G) / \#G_x \equiv 0 [p]$ . Alors  $n = \#H_x \cdot \#G_x$   
 $p$ , premier, est premier avec tout nombre qu'il ne divise pas. Donc  $\Delta(p^k, \#G_x) = 1$   
et le théorème de Gauss donne:  $p^k \mid \#H_x$ .  $H_x$ , stabilisateur de  $x$ , est un sous-groupe de  $G$  d'ordre  $\#H_x = \frac{n}{\#G_x} < n$  puisque  $\#G_x > 1$ .  
D'après l'hyp. de récurrence:  $H_x$  possède un sous-groupe d'ordre  $p^k$

b)  $\forall x \in Z(G) / \#G_x \equiv 0 [p]$ .  
L'équation des classes donne:  
$$\#Z(G) = n - \sum_{x \notin Z(G)} \#G_x \equiv 0 [p]$$

Le centre  $Z(G)$  n'est pas trivial. Comme  $p \mid \#Z(G)$ , il existe selon le th. 1 un élément  $a \in Z(G)$  d'ordre  $p$ . Le groupe  $\langle a \rangle = H$  est d'ordre  $p$ . Il est distingué dans  $G$ , puisque  $H \subset Z(G)$ .

$p^k \mid n \Rightarrow p^{k-1} \mid \#(G/H)$   
D'après l'hypothèse de récurrence,  $\exists K' \subset G/H$   $K'$  sous-groupe d'ordre  $p^{k-1}$   
Soit  $\pi: G \rightarrow G/H$  et  $K = \pi^{-1}(K')$ .  $K \supset H$  et  $\pi|_K: K \rightarrow K'$   
donc  $K/H \cong K' \Rightarrow \#K = p^k$   
CQFD



Def | Soit  $p$  un nombre premier.

- Un  $p$ -groupe (ou groupe  $p$ -primaire) est un groupe fini d'ordre  $p^a$
- Si  $H \subset G$ ,  $H$  est un  $p$ -groupe, on dira que c'est un  $p$ -sous-groupe de  $G$ .
- Si  $H \subset G$  est un  $p$ -sous-groupe de  $G$  de cardinal  $p^n$  où  $p^n$  est la plus grande puissance de  $p$  qui divise  $\#G$ , alors  $H$  sera dit "un  $p$ -sous-groupe de Sylow".

(NB:  $H \subset G$  est un  $p$ -sous-groupe de Sylow si c'est un  $p$ -sous-groupe maximal.)

Co | Soit  $G$  un groupe fini et  $p \in \mathcal{P}$   $p \mid \#G$ . Alors il existe un  $p$ -sous-groupe de Sylow de  $G$ .

① Tout conjugué d'un  $p$ -sous-groupe de Sylow est encore un  $p$ -sous-groupe de Sylow.

[  $H \subset G$   $\#H = p^n$  où  $\#G = n = p^m m$   $\Delta(p, m) = 1$ .  $H' = g H g^{-1} = \tau_g(H)$  où  $\tau_g(x) = g x g^{-1}$  est un automorphisme intérieur.  $\tau_g$  est bijectif, donc conserve le cardinal ].

② Soit  $G$  un groupe abélien fini de cardinal  $n$ .

$$\exists m \in \mathbb{N}^* / \forall g \in G \quad m g = 0 \Rightarrow \exists k \in \mathbb{N} \quad n \mid m^k$$

[ Par récurrence sur  $m$ . Soit  $g \in G$ ,  $g \neq 0$  et  $H = \langle g \rangle$ .  $\#G/H < n$   
 $G/H$  est un groupe, et  $m \bar{g} = 0 \quad \forall \bar{g} \in G/H$ . D'après l'hypothèse de récurrence,  
 $\#G/H \mid m^k$  or  $\#G/H = \frac{\#G}{\#H} = \frac{n}{\#H}$  et  $\#H \mid m$

$$\text{d'où } \frac{n}{\#H} \mid m^k \Leftrightarrow m^k = \lambda \frac{n}{\#H} \quad \text{et } \frac{m}{\#H} = \mu \#H \quad \text{d'où } m^{k+1} = \mu \lambda n \Leftrightarrow n \mid m^{k+1} ]$$

Th 3 | Si  $P$  est un  $p$ -sous-groupe de Sylow d'un groupe fini, alors tout  $p$ -sous-groupe de  $N(P)$  est contenu dans  $P$ .

(Rappel:  $N(H) = \{ g \in G / g H g^{-1} = H \}$  )

preuve: Soit  $R$  un  $p$ -sous-groupe contenu dans  $N(P)$ . Comme  $P \triangleleft N(P)$  et  $R \subset N(P)$   
 $R/P \cap R \cong PR/P$ . Or  $\#(R/P \cap R) = p^\alpha \Rightarrow \#PR/P = p^\alpha$  et a fortiori  $\#(PR) = p^\beta$   
 $PR$  est donc un  $p$ -groupe de  $G$ , et il contient  $P$ . Mais  $P$  est un  $p$ -sous-groupe de Sylow, donc maximal parmi les  $p$ -sous-groupes, d'où  $PR = P \Rightarrow R \subset P$

Th 4 | Soit  $H$  un sous-groupe du groupe fini  $G$

Alors :

$H = p$ -sous-groupe de Sylow  $\Leftrightarrow H =$  maximal dans l'ensemble des  $p$ -groupes de  $G$  ordonné par l'inclusion.

$(\Rightarrow) \#H = p^k$  où  $n = p^k m$   $\Delta(m, p) = 1$ .

Soit  $K$  un  $p$ -sous-groupe de  $G$  contenant  $H$ .  $\#K = p^\alpha$

$$H \subset K \Rightarrow k \leq \alpha$$

$$K \text{ sous-groupe de } G \Rightarrow \alpha \leq k \} \Rightarrow \#K = p^k = \#H \Rightarrow H = K$$

Donc  $H$  est maximal.

$(\Leftarrow)$  notons  $\#H = p^k$ . d'autre part il existe  $K \subset G / \#K = p^k$  où  $m = p^k \cdot m'$   
 $(\Delta(m', p) = 1)$ . considérons  $\Lambda = \{ x \in G / x^{p^k} = e \}$ . alors on rem. que  $\Lambda$  est un  $p$ -sous-groupe de  $G$ , et que  $H \subset \Lambda$ .  $H$  étant maximal, on a donc  $H = \Lambda$ .  
 or  $K \subset \Lambda = H$  d'où (à cause des cardinaux)  $K = H$ ,  $H$  est donc un  $p$ -sous-groupe de Sylow.



On généralise le Th1 précédent :

Th (de Cauchy) Soit  $G$  un groupe fini d'ordre  $n$  et  $p$  un diviseur premier de  $n$ .  $G$  possède un élément d'ordre  $p$ .

preuve: récurrence sur  $\#G = n$ . Si  $n = 2$ ,  $G = \mathbb{Z}/2\mathbb{Z}$  et l'assertion est vraie. Supposons la démontrée pour tout  $m < n$ . Soit  $p \mid n$ ,  $p \in \mathcal{P}$ .

Si  $G = \mathbb{Z}(G)$ , le résultat est vrai (cf. Th1)

Supposons  $G \neq \mathbb{Z}(G)$ . De 2 choses l'une :

a)  $\exists x \in G \setminus \mathbb{Z}(G)$  tel que  $p \mid \#H_x$

(ici,  $H_x = \text{stabilisateur de } x \text{ pour la conjugaison} = \{g \in G \mid g^{-1}xg = x\}$  on le nomme aussi le centralisateur de  $x$ .)

Mais  $x \notin \mathbb{Z}(G) \Rightarrow H_x \subsetneq G \Rightarrow \#H_x < \#G$  et d'après l'hypothèse de récurrence, il existe un élément d'ordre  $p$  dans  $H_x$ , donc dans  $G$ .

b)  $\forall x \in G \setminus \mathbb{Z}(G)$ ,  $p \nmid \#H_x$

Mais  $p \in \mathcal{P}$  divise  $n = \#G = \#G/H_x \cdot \#H_x$  et  $p \nmid \#H_x$ , donc  $p \mid \#G/H_x$  pour tout  $x \notin \mathbb{Z}(G)$

D'après l'équation des classes :

$$\#G = \sum_{x \in A} \#G/H_x = \#\mathbb{Z}(G)$$

donc  $p \mid \#\mathbb{Z}(G)$  et  $\mathbb{Z}(G)$  est commutatif ! Le Th1 nous donne l'existence d'un élément d'ordre  $p$  dans  $\mathbb{Z}(G)$ , donc dans  $G$ .

CQFD

Exemple : Dans  $S_4$ , il y a un élément d'ordre 2 et un d'ordre 3.

En effet :  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ ;  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

Ce théorème permet de donner une équivalence précieuse entre définitions :

Pro | Soit  $G$  un groupe fini. Alors :

$$\#G = p^k \iff \{ \forall x \in G \exists \alpha \in \mathbb{N} \quad p^\alpha x = 0 \}$$

(NB : d'où une autre définition d'un  $p$ -groupe, si  $G$  est un groupe fini. Dans le cas où  $G$  est infini,  $G$  est dit  $p$ -groupe si  $\forall x \in G \exists \alpha \mid \omega(x) = p^\alpha$ , et la définition de "droite" s'avère plus généralisable...)

- Si  $\#G = p^k \quad \forall x \in G \langle x \rangle \subset G \Rightarrow \omega(x) = p^\alpha$  (Th. Lagrange)
- Inversement, si  $\forall x \in G \exists \alpha \quad p^\alpha x = 0$ , supposons que  $q \in \mathcal{P}$   $q \nmid \#G$ . D'après le théorème de Cauchy ci-dessus,  $G$  possède un élément d'ordre  $q$ . Donc  $\exists \alpha \mid q = p^\alpha$  et  $q \in \mathcal{P} \Rightarrow \alpha = 1$ . Ainsi  $q = p \Rightarrow \#G = p^k$ .

### 3° Dénombrement des $p$ -groupes de Sylow

Th 5 | Deux  $p$ -sous-groupes de Sylow d'un groupe fini  $G$  sont conjugués dans  $G$ .  
Le nombre de  $p$ -sous-groupes de Sylow de  $G$  est de la forme  $1 + kp$ .

(NB : on sait déjà que si  $H$  est un  $p$ -sous-groupe de Sylow, alors tous les conjugués de  $H$  sont aussi des  $p$ -sous-groupes de Sylow)

parties :

1<sup>re</sup> partie : On montre que  $\# \mathcal{O} = n \equiv 1 [p]$ 

$G$  opère sur  $\mathcal{H}$  ensemble des sous-groupes de  $G$ , par conjugaison :  $G \times \mathcal{H} \longrightarrow \mathcal{H}$   
 $g, H \longmapsto gHg^{-1}$

 $P$  = sous-groupe de Sylow $N(P) = G_P = \{g \in G / gPg^{-1} = P\}$  = groupe d'isotropie, ou stabilisateur, de  $P$ .(NB: ici, il est égal au normalisateur de  $P$ )On désigne par  $\mathcal{O}$  l'orbite de  $P$ . On a :  $\# \mathcal{O} = n = \frac{\# G}{\# N(P)}$  $P$  opère sur  $\mathcal{O}$  par conjugaison :  $P \times \mathcal{O} \longrightarrow \mathcal{O}$   
 $h, H \longmapsto hHh^{-1}$ Soit  $\mathcal{U}$  l'orbite de  $P$  sous cette action.

$$\mathcal{U} = \{O \in \mathcal{O} / \exists h \ hP h^{-1} = O\} = \{P\}$$

Ainsi  $\# \mathcal{U} = 1$ .Soit  $\mathcal{U}_i$  = orbite de  $P_i \in \mathcal{O}$ , pour  $P_i \neq P$ .Si  $\# \mathcal{U}_i = 1 \Rightarrow hP_i h^{-1} = P_i \ \forall h \in P \Rightarrow P \subset N(P_i)$  et d'après le théorème 3 :  
 $P \subset P_i$  (car  $P$  = p-sous-groupe).Comme  $P$  est maximal dans l'ensemble des p-groupes  $P \subset P_i \Rightarrow P = P_i$ , ce qui est absurde.Donc  $P_i \neq P \Rightarrow \# \mathcal{U}_i \neq 1$ . L'équation des classes donne :

$$\# \mathcal{O} = n = 1 + \sum \# \mathcal{U}_i$$

Notons  $H_i$  le stabilisateur de  $P_i$  sous l'action  $P_i \neq P$  de  $P$  opérant sur  $\mathcal{O}$  par conjugaison :

$$\# \mathcal{U}_i = \frac{\# P_i}{\# H_i} \Rightarrow \# P_i = (\# \mathcal{U}_i)(\# H_i) \Rightarrow \# \mathcal{U}_i \equiv 0 [p]$$

( $\# \mathcal{U}_i \neq 1$  et  $P_i$  = p-sous-groupe de Sylow)

$$\text{d'où } n \equiv 1 [p] \quad (n = \# \mathcal{O}) \quad (1)$$

2<sup>e</sup> partie : Tous les p-sous-groupes de Sylow sont dans  $\mathcal{O}$ .Soit  $Q$  un p-sous-groupe de Sylow non conjugué à  $P$ . Cela revient à dire que  $Q \notin \mathcal{O}$  $Q$  opère par conjugaison sur  $\mathcal{O}$ 

$$Q \times \mathcal{O} \longrightarrow \mathcal{O}$$

$$(q, O) \longmapsto qOq^{-1}$$

Si  $\mathcal{V}_i$  = orbite de  $P_i \in \mathcal{O}$ , alors  $\forall P_i \in \mathcal{O} : \# \mathcal{V}_i \neq 1$ 

$$[\# \mathcal{V}_i = 1 \Rightarrow \forall q \in Q \ qP_i q^{-1} = P_i \Rightarrow Q \subset N(P_i) \Rightarrow Q \subset P_i]$$

donc  $Q = P_i$  (cf  $Q$  maximal)

(th3)

Donc  $\# \mathcal{V}_i \neq 1$ 

$$\text{L'équation des classes est ici : } \# \mathcal{O} = \sum \# \mathcal{V}_i \quad \text{où } \# \mathcal{V}_i = \frac{\# Q}{\# (\text{stabilisateur de } P_i)}$$

$$\# \mathcal{V}_i \neq 1 \Leftrightarrow \# \mathcal{V}_i > 1 \Rightarrow \# Q > \# (\text{stabilisateur de } P_i)$$

Comme  $\# Q = p^n$  et que (stabilisateur de  $P_i$ )  $\subset Q$  est de cardinal  $p^x$ , et comme  $p^n > p^x$ , on en déduit que  $\# \mathcal{V}_i \equiv 0 [p]$ .

$$\text{Donc } \# \mathcal{O} = \sum \# \mathcal{V}_i \equiv 0 [p] \quad \text{ce qui est absurde selon (1)!}$$

Conclusion :  $Q$  = p-sous-groupe de Sylow  $\Rightarrow Q \in \mathcal{O}$  (orbite de  $P$ )  
 et  $\# \mathcal{O} = n \equiv 1 [p]$ .

Pro | Soit  $G$  un  $p$ -groupe.  
 1) Alors  $Z(G) \neq \{e\}$   
 2)  $G$  est résoluble.

preuve: 1) On considère l'équation des classes pour l'opération de conjugaison:

$$G \times G \rightarrow G$$

$$(g, x) \mapsto g x g^{-1}$$

$$\# G = \# Z(G) + \sum_{x \in A} \frac{\# G}{\# H_x}$$

Comme  $\# G = p^n$ ,  $G_x \subset G \Rightarrow \# G_x \mid p^n$   
 et  $\# G_x \neq p^n$  (sinon  $G_x = G$  et  $Z(G) = G$ !) Donc  $\# Z(G) \equiv 0 \pmod{p}$ . (1)

2)  $G$  est résoluble.

Récurrence sur  $\# G$ .

- vrai pour  $\# G = 2$  car  $G = \mathbb{Z}/2\mathbb{Z}$  résoluble car commutatif.
- $Z(G) \subset G$  est un sous-groupe de  $G$  et  $\# G/Z(G) < \# G$  d'après (1)

Alors:

$$G/Z(G) = G'_0 \supset G'_1 \supset \dots \supset G'_n = \{e\} \quad (2)$$

où  $G'_{k+1} \triangleleft G'_k$  et  $G'_k/G'_{k+1}$  commutatif

Notons  $\pi: G \rightarrow G/Z(G)$ . On pose  $G_i = \pi^{-1}(G'_i)$ . On sait que  $\pi$  est une bijection croissante de l'ensemble des sous-groupes contenant  $Z(G)$  sur l'ensemble des sous-groupes de  $G/Z(G)$ . Ainsi (2)  $\Rightarrow$

$$G = G_0 \supset G_1 \supset \dots \supset G_n = \pi^{-1}(\{e\}) = Z(G)$$

$$\text{et } \begin{cases} \bullet G_{k+1} \triangleleft G_k \\ \bullet G_k/G_{k+1} \cong G'_k/G'_{k+1} \end{cases}$$

CQFD

[NB: •  $\forall x \in G_k \forall g \in G_{k+1} \overline{x g x^{-1}} \in G'_{k+1} \Rightarrow \overline{x g x^{-1}} = \overline{g'} \quad g' \in G'_{k+1}$   
 c.d.d  $\overline{x g x^{-1}} \overline{g'^{-1}} \in Z(G) \subset G_{k+1} \Rightarrow \overline{x g x^{-1}} \in G_{k+1}$ .

• Considérons  $\pi: G_i/G_{i+1} \longrightarrow G'_i/G'_{i+1}$ . C'est un isomorphisme.  
 $\pi \longmapsto \overline{\pi(x)}$

\*  $\pi$  est bien définie car  $\overline{x} = \overline{y} \Leftrightarrow x y^{-1} \in G_{i+1} \Rightarrow \pi(x) \pi(y)^{-1} \in G'_{i+1} \Leftrightarrow \overline{\pi(x)} = \overline{\pi(y)}$

\*  $\pi$  surjective.

\*  $\pi$  injective: car  $\left\{ \begin{array}{l} \overline{\pi(x)} = \overline{0} \\ x \in G_i \end{array} \right\} \Leftrightarrow \pi(x) \in G'_{i+1} \Leftrightarrow x \in G_{i+1} \Rightarrow \overline{x} = \overline{0}$ . ]



# Décomposition d'un groupe commutatif fini

(Dany-Jack MERCIER, 1979)

[Ligne - décomposition d'un groupe commutatif fini].pdf

## I Définition d'un p-groupe

Def | Soit  $G$  un groupe. On dit que  $G$  est un  $p$ -groupe si son cardinal est une puissance de  $p$  ( $p \in \mathbb{P}$ ).

Th | Soit  $G$  un groupe commutatif fini.  
Alors  $G = p$ -groupe  $\Leftrightarrow \{ \forall x \in G \exists \alpha \in \mathbb{N} / \omega(x) = p^\alpha \}$

preuve: • Supposons que  $\forall x \in G \omega(x) = p^\alpha$ . On fait une récurrence sur le cardinal de  $G$ . En notation additive:

→ Pour  $G = \{0\}$ , c'est évident

→ Soit  $G$  de cardinal  $n$ . Soit  $x \in G$ ,  $x \neq 0$ . Notons  $H = \langle x \rangle$ . C'est un groupe cyclique d'ordre  $p^k$ . Mais  $\#G = \#H \cdot \#G/H$  et  $G/H$ , groupe commutatif, vérifie  $\forall \bar{x} \in G/H \exists \alpha / p^\alpha \bar{x} = 0$ . De plus  $\#G/H < \#G$ . L'hypothèse de récurrence s'applique:  $\#G/H = p^\beta$ . Comme  $\#H = p^k$ , on trouve que  $\#G = p^{\beta+k}$  cqfd  
• Inversement, si  $G$  est un  $p$ -groupe,  $\#G = p^k$  et tout élément  $x$  de  $G$  engendre  $\langle x \rangle$  d'ordre  $p^\alpha \mid p^k$ . Par suite  $\omega(x) = p^\alpha$ .

## II Décomposition en p-groupes (ou "composantes p-primaires")

Th | Soit  $G$  un groupe commutatif fini d'ordre  $n = p_1^{n_1} \dots p_k^{n_k} = q_1 \dots q_k$   
Posons  $G(p_i) = \{x \in G / q_i x = 0\}$   
 $G(p_i)$  est un  $p_i$ -groupe et:

$$G = G(p_1) \oplus \dots \oplus G(p_k)$$

Il est clair que  $G(p_i)$  est un groupe, et que  $\forall x \in G(p_i) \omega(x) \mid p_i^{n_i} \Rightarrow \omega(x) = p_i^{\alpha}$   
donc  $G(p_i) = p_i$ -groupe.

Montrons la somme directe:

$$\forall x \in G \exists x_i \in G(p_i) / x = x_1 + \dots + x_k \quad ?$$

$$\text{Il est clair que } \Delta\left(\frac{n}{q_1}, \frac{n}{q_2}, \dots, \frac{n}{q_k}\right) = 1 \Leftrightarrow \sum_{i=1}^k m_i \frac{n}{q_i} = 1 \quad (\text{Bezout})$$

$$\text{Donc } x = \underbrace{m_1 \frac{n}{q_1} x}_{\in G(p_1)} + \dots + \underbrace{m_k \frac{n}{q_k} x}_{\in G(p_k)}$$

$$\text{Donc } G = G(p_1) + \dots + G(p_k)$$

$$\forall j \in [1, k] \quad G(p_1) + \dots + G(p_{j-1}) \cap G(p_j) = \{0\} \quad ?$$

$$\text{Soit } x \in G(p_1) + \dots + G(p_{j-1}) \cap G(p_j) \text{ où } j \in [1, k]$$

$$\text{Alors } q_j x = 0 \text{ et } x = x_1 + \dots + x_{j-1} \text{ où } x_i \in G(p_i) \Leftrightarrow q_i x_i = 0 \quad \forall i$$

$$\text{Soit } s = \prod_{i=1}^{j-1} q_i. \text{ On a } sx = 0$$

$$q_j \text{ et } s \text{ sont premiers entre eux! donc } \lambda q_j + \mu s = 1 \Rightarrow x = \lambda q_j x + \mu s x = 0$$

CQFD

## composition en p-groupes cycliques. (2)

Enons tout d'abord :

**Th 1** Tout p-groupe commutatif G se décompose en groupes cycliques p-primaires,  

$$G \cong \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{\alpha_s}\mathbb{Z} \quad \alpha_1 \leq \dots \leq \alpha_s$$
  
 De plus, la suite  $(\alpha_1, \dots, \alpha_s)$  est unique.

Soit G un p-groupe commutatif. Enons 2 lemmes :

lemme 1 :  $b \in G \quad b \neq 0 \quad p^k b \neq 0 \quad \left. \begin{array}{l} \omega(p^k b) = p^m \\ \omega(b) = p^{m+k} \end{array} \right\} \Rightarrow \omega(b) = p^{m+k}$

lemme 2 : Soit  $a_1 \in G \quad G_1 = \langle a_1 \rangle / \pi G_1 = p^{n_1} = \sup \{ \omega(x) / x \in G \}$   
 Soit  $\bar{b} \in G/G_1$  tel que  $\omega(\bar{b}) = p^n$ . On pose  $\pi_1: G \rightarrow G/G_1$   
 Alors  $\exists b / \pi_1(b) = \bar{b}$  et  $\omega(b) = p^n$ .

preuve lemme 1 : On a  $\left\{ \begin{array}{l} p^{m+k} b = 0 \\ p^{m+k-1} b = p^{m-1} (p^k b) \neq 0 \text{ car } \omega(p^k b) = p^m \quad (m \geq 1) \end{array} \right.$   
 donc  $\omega(b) = p^{m+k}$

preuve lemme 2 : Soit  $b \in G$  tel que  $\pi_1(b) = \bar{b}$ .  $\pi_1$  est un morphisme de groupes, donc il abaisse les ordres des éléments :  $\omega(b) \geq p^n, \forall b \in \pi_1^{-1}(\bar{b})$ . (x)

On a  $p^k b \in G_1 \Leftrightarrow p^k b = n a_1$  où  $0 \leq n < p^{n_1}$   
 $p^k b = p^k \mu a_1$  où  $p \nmid \mu$  ( $k < n_1$ )  
 $\omega(p^k \mu a_1) = \frac{p^{n_1}}{\Delta(p^k \mu, p^{n_1})} = p^{n_1-k}$  et  $p^k b \neq 0 \Rightarrow \omega(b) = p^{n_1-k}$  (lemme 1)

Comme  $n_1 = \sup \{ \omega(x) / x \in G \}$  et que  $\omega(b) = p^{n_1-k}$ , on aura forcément l'inégalité :  $n_1 - k \leq n_1 \Leftrightarrow k \geq 0$   
 Par suite :  $p^k b = p^k \mu a_1 \Rightarrow (b - p^{k-1} \mu a_1) p^n = 0 \Rightarrow \omega(b - p^{k-1} \mu a_1) = p^n$   
 On a qu'à prendre  $b' = b - p^{k-1} \mu a_1 \in \pi_1^{-1}(\bar{b})$  (cf. (x))

preuve du théorème :

### • Existence de la décomposition

$\pi G = p^u$ . On fait une récurrence sur u.

C'est vrai pour  $u=1$ . Soit G de cardinal  $\pi G = p^u$ . Alors  $\pi G/G_1 = p^{u-n_1}$  et l'on peut appliquer l'hypothèse de récurrence :

$$G/G_1 = \bar{G}_2 \oplus \dots \oplus \bar{G}_s \quad \text{où} \quad \bar{G}_i = \bar{a}_i \mathbb{Z} \quad \omega(\bar{a}_i) = p^{n_i} \quad (\text{groupes cycliques primaires})$$

D'après le lemme 2 :

$$\exists a_i \in G \quad / \quad \pi(a_i) = \bar{a}_i \quad \text{et} \quad \omega(a_i) = p^{n_i}$$

Prenons  $G_i = a_i \mathbb{Z} = \langle a_i \rangle$  et montrons que  $G = G_1 \oplus \dots \oplus G_s$  :  $a_i \in G_i$

1)  $G = G_1 + \dots + G_s$

En effet,  $\forall x \in G \quad x = m_1 a_1 + \dots + m_s a_s \Leftrightarrow x = m_1 a_1 + \dots + m_s a_s$

2) Si  $m_1 a_1 + \dots + m_s a_s = 0 \quad 0 \leq m_i < p^{n_i}$

alors  $m_2 a_2 + \dots + m_s a_s = 0$  d'où  $m_2 = \dots = m_s = 0$  et  $m_1 a_1 = 0 \Rightarrow m_1 = 0$

Donc  $G = G_1 \oplus \dots \oplus G_s \quad G_i = \text{groupe cyclique primaire d'ordre } p^{n_i}$

### • Unicité de la suite $(\alpha_1, \dots, \alpha_s)$

$$\text{On a } G \cong (\mathbb{Z}/p\mathbb{Z})^{m_1} \times \dots \times (\mathbb{Z}/p^t\mathbb{Z})^{m_t}$$

Montrons que cette décomposition est unique.

$$G(p) \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \times \dots \times (\mathbb{Z}/p^r\mathbb{Z})^{m_r}$$

(3)

$$G(p) \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \times p(\mathbb{Z}/p^2\mathbb{Z})^{m_2} \times \dots \times p^{t-1}(\mathbb{Z}/p^t\mathbb{Z})^{m_t}$$

(où  $G[p] = \{x \in G / px = 0\} = "$  p-groupe élémentaire de  $G$  " = groupe d'ordre  $p$ .)

Mais pour  $h \in \mathbb{R}$   $p^h(\mathbb{Z}/p^h\mathbb{Z}) = 0$ . Donc :

$$p^k G \simeq p^k(\mathbb{Z}/p^{k+1}\mathbb{Z})^{m_{k+1}} \times \dots \times p^k(\mathbb{Z}/p^t\mathbb{Z})^{m_t}$$

$$\simeq (p^k\mathbb{Z}/p^{k+1}\mathbb{Z})^{m_{k+1}} \times \dots \times (p^k\mathbb{Z}/p^t\mathbb{Z})^{m_t}$$

$$\text{donc } p^k G \cap G[p] = (p^k\mathbb{Z}/p^{k+1}\mathbb{Z})^{m_{k+1}} \times \dots \times (p^k\mathbb{Z}/p^t\mathbb{Z})^{m_t} \quad \left\{ \begin{array}{l} \text{je ne vois pas pourquoi} \\ \text{ce j'aurais pu.} \\ \text{cf Alternative possible} \\ \text{qui n'utilise que } p^k G \end{array} \right.$$

Comme, d'autre part  $(p^k\mathbb{Z}/p^{i+1}\mathbb{Z}) / (p^i\mathbb{Z}/p^{i+1}\mathbb{Z}) \simeq p^k\mathbb{Z}/p^i\mathbb{Z}$

et comme, dans un groupe commutatif  $(H \times H') / (K \times K') \simeq H/K \times H'/K'$  (cf. 2.12 boursier), on obtient :

$$\begin{aligned} p^k G \cap G[p] / p^{k+1} G \cap G[p] &\simeq (p^k\mathbb{Z}/p^{k+1}\mathbb{Z})^{m_{k+1}} \\ &\simeq (\mathbb{Z}/p\mathbb{Z})^{m_{k+1}} \end{aligned}$$

p-groupe élémentaire. C'est donc un espace vectoriel sur  $\mathbb{Z}/p\mathbb{Z}$ .  
On voit ici qu'il est de dimension  $m_{k+1}$ . Ainsi :

$$m_{k+1} = \dim_{\mathbb{Z}/p\mathbb{Z}} p^k G \cap G[p] / p^{k+1} G \cap G[p] \quad \text{qui ne dépend que de } k \text{ et de } G.$$

$m_{k+1}$  est donc indépendant de la décomposition choisie.

$$\text{Ainsi : } G \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \times \dots \times (\mathbb{Z}/p^t\mathbb{Z})^{m_t} \simeq (\mathbb{Z}/p\mathbb{Z})^{m'_1} \times \dots \times (\mathbb{Z}/p^{t'}\mathbb{Z})^{m'_{t'}} \quad (t \leq t')$$

Un argument de "cardinal" montre que  $p^{m'_1} + \dots + t m'_t = p^{m_1} + \dots + t m_t$ ,  
donc que  $(t+1)m'_{t+1} + \dots + t'm'_t = 0 \Rightarrow m'_{t+1} = \dots = m'_{t'} = 0$ .

CQFD

Th2 Soit  $G$  un groupe fini commutatif d'ordre  $n = p_1^{a_1} \dots p_k^{a_k}$ .  
 $G$  est décomposable en groupes cycliques primaires, et  
l'on a :

$$G \simeq \mathbb{Z}/p_1^{a_{11}}\mathbb{Z} \times \mathbb{Z}/p_1^{a_{12}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_1^{a_{1n_1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{a_{k1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{a_{kn_k}}\mathbb{Z}$$

$$\text{où } \begin{cases} p_1 < p_2 < \dots < p_k \\ a_{i1} \leq \dots \leq a_{in_i} \end{cases}$$

La suite  $(p_1^{a_{11}}, \dots, p_1^{a_{1n_1}}, \dots, p_k^{a_{k1}}, \dots, p_k^{a_{kn_k}})$  est parfaitement déterminé. Il se nomme "le type de  $G$ ".

Ce théorème nous révèle la structure de tout groupe commutatif fini.  
Il se démontre en utilisant le théorème de décomposition en groupes primaires.

⊛ Alternative : Pourquoi parler de  $G[p]$  ? Certains résultats restent à justifier ci-dessus au ⊛, alors utilisons seulement :

$$p^k G \cong \left( p^k \mathbb{Z} / p^{k+1} \mathbb{Z} \right)^{m_{k+1}} \times \left( p^k \mathbb{Z} / p^{k+2} \mathbb{Z} \right)^{m_{k+2}} \times \dots \times \left( p^k \mathbb{Z} / p^t \mathbb{Z} \right)^{m_t}$$

pour obtenir :

$$\begin{aligned} p^k G / p^{k+1} G &\cong \left( p^k \mathbb{Z} / p^{k+1} \mathbb{Z} \right)^{m_{k+1}} \times \left( p^k \mathbb{Z} / p^{k+1} \mathbb{Z} \right)^{m_{k+2}} \times \dots \times \left( p^k \mathbb{Z} / p^{k+1} \mathbb{Z} \right)^{m_t} \\ &\cong \left( \mathbb{Z} / p \mathbb{Z} \right)^{m_{k+1} + \dots + m_t} \end{aligned}$$

C'est encore un e.v. sur le corps  $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ , soit :

$$m_{k+1} + \dots + m_t = \dim_{\mathbb{F}_p} \left( p^k G / p^{k+1} G \right)$$

Cette dernière dim. est dépendante de  $G$  et de  $k$  uniquement, et l'égalité précédente permet d'obtenir successivement  $m_t, m_{t-1}, \dots, m_1$  à partir de ces dimensions : l'unicité de  $m_1, m_2, \dots, m_t$  est donc établie. (—)

Pour conclure, considérons encore :

$$G \cong \left( \mathbb{Z}/p\mathbb{Z} \right)^{m_1} \times \dots \times \left( \mathbb{Z}/p^t \mathbb{Z} \right)^{m_t} \cong \left( \mathbb{Z}/p\mathbb{Z} \right)^{m'_1} \times \dots \times \left( \mathbb{Z}/p^{t'} \mathbb{Z} \right)^{m'_{t'}}$$

On peut toujours supposer que ~~max~~  $t = t'$  quitte à rajouter des  $m_i$  nuls.

Vu ce qui précède, on aura :

$$\begin{cases} m_t = m'_{t'} \\ \dots \\ m_1 = m'_1 \end{cases}$$

CPFH

$$G = G(p_1) \oplus \dots \oplus G(p_k) \quad (\text{cf paragraphe 1})$$

(4)

en utilisant le Th 1 ci-dessus:

$$G(p_i) \cong \mathbb{Z}/\alpha_{i,1}\mathbb{Z} \times \dots \times \mathbb{Z}/\alpha_{i,n_i}\mathbb{Z}$$

L'unicité de la décomposition  $(p_1^{n_1}, \dots, p_k^{n_k})$ , qui détermine le type de  $G$ , est dû:

a) à l'unicité de la suite du Th. 1 :  $(p_1^{\alpha_{1,1}}, \dots, p_k^{\alpha_{k,n_k}})$  est unique.

b) à la remarque suivante :  $G = G(p_1) \oplus \dots \oplus G(p_k)$

Si  $G_i$  est  $p_i$ -primaire cyclique, alors  $\forall x \in G_i$   $p_i^{\#G_i} x = 0$ , donc  $x \in G(p_i) = \{x \in G / p_i^{\#G_i} x = 0\}$ . Ainsi  $G_i \subset G(p_i)$

CQFD

Application :

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  est de type  $(2, 2)$

$\mathbb{Z}/4\mathbb{Z}$  est de type  $(2^2)$

$G = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z}$  est de type  $(2^3, 2^4, 3^2, 5^3)$

Remarque :  $G$  est d'ordre  $2^2 \times 3^2 \times 5^3 = 14400$  et de type  $(2^3, 2^4, 3^2, 5^3)$   
Le type  $(2^3, 2^4, 3^2, 5^3)$  ne doit pas être confondu avec le  $k$ -uplet  $(p_1^{n_1}, \dots, p_k^{n_k})$  de la décomposition de  $n$  en facteurs premiers.

Toutefois, puisque  $n = \#G = \prod_{\substack{i=1, k \\ j=1, n_i}} \#(\mathbb{Z}/\alpha_{i,j}\mathbb{Z})$ , on trouve que :

$$\begin{cases} n_1 = \sum_{j=1}^{n_1} \alpha_{1,j} \\ \dots \\ n_k = \sum_{j=1}^{n_k} \alpha_{k,j} \end{cases}$$

$$\text{où } n = p_1^{n_1} \dots p_k^{n_k}$$

Co | Deux groupes abéliens finis sont isomorphes si ils ont même type.

preuve : Si  $G$  et  $G'$  ont même type, il est clair qu'ils sont isomorphes.  
Inversement, si  $G \cong G'$ , soit  $G = \bigoplus_{i=1}^m \Gamma_i$  et  $G' = \bigoplus_{i=1}^{m'} \Gamma'_i$  les décompositions de  $G$  et  $G'$  en groupes cycliques primaires.  
 $\exists \Phi: G \xrightarrow{\sim} G'$ . Alors  $\bigoplus_{i=1}^m \Phi(\Gamma_i)$  est une décomposition de  $G'$  en groupes cycliques primaires.  
d'après l'unicité des types,  $m = m'$  et les types de  $G$  et de  $G'$  sont les mêmes.



$A$  désigne une partie non vide d'un groupe  $G$ .

$N(A) = \{x \in G \mid xAx^{-1} = A\}$  = normalisateur de  $A$  dans  $G$ .

$C(A) = \{x \in G \mid \forall a \in A \quad ax = xa\}$  = centralisateur de  $A$  dans  $G$ .

a) Hq  $N(A)$  est un sous-groupe de  $G$ , et que  $C(A) \trianglelefteq N(A)$

b) Soit la relation:  $x \mathcal{R} y \Leftrightarrow xax^{-1} = yay^{-1}$  <sup>(où  $a \in G$  est fixé)</sup>. Hq  $\mathcal{R}$  est une relation d'équivalence, puis montrer que si  $G$  est fini, le cardinal de l'ensemble des conjugués de  $a \in G$  est égal à l'indice du normalisateur de  $\{a\}$  dans  $G$ .  
(Rappel:  $b \in G$  est un conjugué de  $a$  s'il existe  $x \in G \mid b = xax^{-1}$ )

a)  $e \in N(A) \cap C(A)$  donc  $N(A)$  et  $C(A)$  ne sont pas vides.

Si  $x, y \in N(A)$ ,  $xy^{-1}A(xy^{-1})^{-1} = xy^{-1}Ayx^{-1} = xAx^{-1} = A$  entraîne  $xy^{-1} \in N(A)$ , ie  $N(A)$  sous-groupe de  $G$ .

$C(A) \subset N(A)$  et si  $x, y \in C(A)$ , on a:  $\forall a \in A \quad axy^{-1} = xay^{-1} = x y^{-1}a$  donc  $xy^{-1} \in C(A)$ .  $C(A)$  est donc un sous-groupe de  $N(A)$ .

\*  $C(A) \trianglelefteq N(A)$ ?

1<sup>re</sup> méthode:  $\forall x \in C(A) \quad \forall y \in N(A) \quad yxy^{-1} \in C(A)$ ?

On a:

$$\forall a \in A \quad a(yxy^{-1}) = ayxy^{-1} = y a' x y^{-1} = y x a' y^{-1} = y x y^{-1} a \quad \text{d'où } yxy^{-1} \in C(A)$$

$\uparrow$   $yA = Ay$  donc  $\exists a' \in A \mid ay = ya'$   $\uparrow$  car  $ay = ya' \Rightarrow y'a = a'y^{-1}$

2<sup>ème</sup> méthode: Soit  $\beta_x \in \mathcal{I}(G)$  l'automorphisme intérieur défini par  $\beta_x(a) = xax^{-1}$

Si  $x \in N(A)$ ,  $\beta_x(A) \subset A$  et l'on peut définir le morphisme de groupes:

$$\begin{aligned} \varphi: N(A) &\longrightarrow (\mathcal{I}(A), \circ) \\ x &\longmapsto \beta_x \end{aligned}$$

le noyau  $\text{Ker } \varphi = C(A)$ , donc  $C(A) \trianglelefteq N(A)$ .

b)  $\mathcal{R}$  est clairement une relation d'v, et les classes d'équivalences par  $\mathcal{R}$  ont en nbre égal au nbre de conjugués de  $a$ .

Comme:  $x \mathcal{R} y \Leftrightarrow xax^{-1} = yay^{-1} \Leftrightarrow ax^{-1}y = x^{-1}ya \Leftrightarrow x^{-1}y \in C(\{a\}) = N(\{a\})$

$$G/\mathcal{R} = \frac{G}{C(\{a\})} \quad (\text{classes à gauche suivant } C(\{a\})), \text{ d'où } \# \frac{G}{\mathcal{R}} = \underbrace{[G : C(\{a\})]}_{\substack{\text{nbre de} \\ \text{conjugués de } a}} \quad \underbrace{[G : C(\{a\})]}_{\substack{\text{indice de } C(\{a\}) \\ \text{dans } G}}$$

(NB: cf VRamis ex Alg n° 2.1.10)

Soit  $G$  un groupe à 6 éléments.

a) Si  $G$  est commutatif, alors  $G \cong \mathbb{Z}/6\mathbb{Z}$

b) Si  $G$  n'est pas commutatif, alors  $G \cong S_3$

a) Supposons, par l'absurde, qu'il n'existe aucun élément de  $G$  d'ordre 6. L'ordre d'un élément  $a \neq e$  de  $G$  sera donc 2 ou 3 (Lagrange).

\* Tous les éléments de  $G$  ne peuvent être d'ordre 2 :

Si  $H_1 = \langle a \rangle = \{e, a\}$  et  $H_2 = \langle b \rangle = \{e, b\}$  permettent de parler du sous-groupe  $\{e, a, b, ab\}$  d'ordre 4, et 4 ne divise pas 6. Absurde.

\* Tous les éléments de  $G$  ne peuvent être d'ordre 3 :

Si on fixe  $a \in G \setminus \{e\}$  d'ordre 3,  $\langle a \rangle = \{e, a, a^2\}$  et  $b \in G \setminus \langle a \rangle$ .

$b$  sera d'ordre 3 et  $\langle b \rangle = \{e, b, b^2\}$  vérifiera  $\langle a \rangle \cap \langle b \rangle = \{e\}$

(sinon  $a^2 = b^2 \Rightarrow e = b^2 a \Rightarrow b = a$  faux ; et  $a = b^2 \Rightarrow ab = e \Rightarrow b = a^2$  faux car  $b \in G \setminus \langle a \rangle$ )

Alors  $G = \{e, a, a^2, b, b^2, x\}$  et le dernier élément  $x$  ne peut qu'être d'ordre 2 (car  $\langle x \rangle \cap \langle a \rangle$  sous-groupe de  $\langle a \rangle$  sera d'ordre 3 ou 1. Si

$\# \langle x \rangle \cap \langle a \rangle = 3$ ,  $\langle x \rangle = \langle a \rangle \Rightarrow x \in \langle a \rangle$  absurde. Donc  $\# \langle x \rangle \cap \langle a \rangle = 1$

ie ( $\langle x \rangle \cap \langle a \rangle = \{e\}$ ). De même pour  $b$ . Finalement  $\langle x \rangle = \{e, x\}$  car  $\langle x \rangle \cap \langle a \rangle = \{e\}$  et  $\langle x \rangle \cap \langle b \rangle = \{e\}$ )

\* Finalement, il existe un élément  $a$  d'ordre 2 et un élément  $b$  d'ordre 3 dans  $G$ . Alors  $ab$  sera d'ordre 6 comme le montre le calcul :

$$ab = e \Rightarrow a = b \text{ faux}$$

$$(ab)^2 = a^2 b^2 = b^2 \neq e$$

$$(ab)^3 = a \neq e$$

$$(ab)^4 = b \neq e$$

$$(ab)^5 = a b^2 \neq e \text{ sinon } b = a$$

$$(ab)^6 = e$$

$\omega(ab) = 6$  est l'absurdité cherchée !

b) Tout groupe dont tous les éléments sont d'ordre 2 est commutatif (en effet :  $(ab)^2 = e = a^2 b^2 \Rightarrow abab = a^2 b^2 \Rightarrow ba = ab$ ).  $G$  n'étant pas commutatif, il existe un élément  $a \in G$  d'ordre 3.

Soient  $\langle a \rangle = \{e, a, a^2\}$  et  $b \in G \setminus \langle a \rangle$ .

\* Le sous-groupe engendré par  $a$  et  $b$  a un ordre  $\geq 4$ , donc est égal à  $G$ .

\*  $a$  et  $b$  ne commutent pas, sinon  $H = G$  serait commutatif.

\* Si  $b$  était d'ordre 3,  $a^2$  et  $b^2$  seraient distincts de  $e, a, b, ab, ba$ , ce qui est absurde puisque  $G$  possède seulement 6 éléments.

Donc  $b$  est d'ordre 2.

\* Comme  $a^2 \notin \{e, a, b, ab, ba\}$ , on en déduit  $G = \{e, a, a^2, b, ab, ba\}$

puis la table :

	$e$	$a$	$a^2$	$b$	$ab$	$ba$
$e$	$e$	$a$	$a^2$	$b$	$ab$	$ba$
$a$	$a$	$a^2$	$e$	$ab$	$ba$	$b$
$a^2$	$a^2$	$e$	$a$	$ba$	$b$	$ab$
$b$	$b$	$ba$	$ab$	$e$	$a^2$	$a$
$ab$	$ab$	$b$	$ba$	$a$	$e$	$a^2$
$ba$	$ba$	$ab$	$b$	$a^2$	$a$	$e$

(Remplir les cases faciles puis s'arranger pour que tous les él. d'une ligne ou d'une colonne soient distincts!)

← colonne ou ligne d'où la fin du tableau

C'est la table de  $S_3$  avec :

$$e = Id \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2, 3)$$

$$a^2 = (1, 2, 3)$$

$$a^2 = (1, 3, 2) \quad \text{etc}$$

Soit  $n \geq 3$ . On désigne par  $\mathcal{A}'_n$  le sous-groupe de  $\mathcal{S}_n$  engendré par les cycles  $(1, 2, 3)$ ,  $(1, 2, 4)$ ,  $\dots$ ,  $(1, 2, n)$ .

1° Montrer que  $\mathcal{A}'_n$  est un sous-groupe de  $\mathcal{A}_n$

2° Montrer que si  $i, j$  sont 2 entiers distincts appartenant à  $\mathcal{M}_n$ , les permutations  $(1, 2)(i, j)$  et  $(i, j)(1, 2)$  appartiennent à  $\mathcal{A}'_n$

3° En déduire que  $\mathcal{A}'_n = \mathcal{A}_n$ . On remarquera que toute permutation  $\sigma$  de  $\mathcal{A}_n$  s'écrit sous la forme  $\sigma = \tau_1 \tau_2 \dots \tau_{2p} = \tau_1 \sigma_0 \sigma_0 \tau_2 \dots \tau_{2p} \sigma_0 \sigma_0 \tau_{2p}$  où  $\sigma_0 = (1, 2)$  et  $\tau_1, \tau_2, \dots, \tau_{2p}$  sont des transpositions.

1°  $\sigma_j = (1, 2, j)$  est un cycle d'ordre 3. Le nombre d'orbites de  $\sigma_j$  est donc  $p = (n-3)+1 = n-2$  et sa signature  $\varepsilon(\sigma_j) = (-1)^{n-p} = (-1)^2 = 1$  i.e.  $\sigma_j \in \mathcal{A}_n$

2° Supposons  $i < j$ .

\* Si  $i=1$  et  $j=2$ ,  $(i, j)(1, 2) = (1, 2)(i, j) = \text{Id} \in \mathcal{A}'_n$

\* Si  $i=1$  et  $j>2$ ,  $(1, 2)(1, j) = (1, j, 2) = (1, 2, j)^2 \in \mathcal{A}'_n$   
 $(1, j)(1, 2) = (1, 2, j) \in \mathcal{A}'_n$

\* Si  $i=2$  et  $j>2$ ,  $(1, 2)(2, j) = (1, 2, j) \in \mathcal{A}'_n$   
 $(2, j)(1, 2) = (1, j, 2) = (1, 2, j)^2 \in \mathcal{A}'_n$

\* Si  $i>2$  et  $j>2$ , les supports de  $(i, j)$  et  $(1, 2)$  sont disjoints, donc  $(i, j)$  et  $(1, 2)$  commutent et :

$$(1, 2)(i, j) = (i, j)(1, 2) = (1, 2, i)(1, 2, j)^2(1, 2, i) \in \mathcal{A}'_n$$

3° Toute permutation  $\sigma$  de  $\mathcal{A}_n$  s'écrivant  $\sigma = (\tau_1 \sigma_0)(\sigma_0 \tau_2) \dots (\sigma_0 \tau_{2p})$  puisque  $\sigma_0^2 = \text{Id}$ , le 2° montrant que si  $\tau$  est une transposition,  $\tau \sigma_0$  et  $\sigma_0 \tau$  sont dans  $\mathcal{A}'_n$ , on en déduit  $\mathcal{A}_n \subset \mathcal{A}'_n$ . Finalement,  $\mathcal{A}'_n = \mathcal{A}_n$ .

① Soit un ensemble muni d'une loi de comp. interne associative notée multiplicativement. On suppose que :

$$a) \exists e \in E \quad \forall x \in E \quad xe = x$$

$$b) \forall x \in E \quad \exists y \in E \quad xy = e$$

$Mq (E, \cdot)$  est un groupe

② A et B étant 2 sous-groupes d'un groupe G, soit S le sous-groupe de G engendré par  $A \cup B$ . a)  $Mq$  S est l'ensemble des éléments de la forme  $x_1 x_2 \dots x_{2n+1}$  où  $n \in \mathbb{N}$ ,  $x_{2i} \in A$  et  $x_{2i+1} \in B$  pour  $i \in [0, n]$ .  
b)  $S = AB \Leftrightarrow AB = BA$

③ Tout sous-groupe H d'indice 2 d'un groupe G est distingué.

① \* Tout x possède un inverse (à dr et à gauche) :

de b) assure déjà l'existence d'un inverse à droite y de x :  $xy = e$   
y possède aussi un inverse à droite :  $\exists z \in E \quad yz = e$

$$\text{Alors : } \underbrace{xy}_e z = ez \Rightarrow x = ez \quad \text{puis} \quad yx = y(ez) = (ye)z = yz = e$$

et y sera aussi inverse à gauche de x.

\* e est élément neutre de E :

Le a) assure déjà que e est neutre à droite. On a :

$$\forall x \in E \quad ex = (xy)x = x(yx) = xe = x \quad \text{d'où la conclusion.}$$

② a) Tout groupe contenant  $A \cup B$  contiendra tous les éléments de la forme  $x_1 x_2 \dots x_{2n+1}$  où  $x_{2i} \in A$  et  $x_{2i+1} \in B$ , donc  $S = \{x_1 x_2 \dots x_{2n+1} / x_{2i} \in A \text{ et } x_{2i+1} \in B\}$ .

Il suffit de prouver que S est un sous-groupe de G pour pouvoir affirmer que S est le plus petit sous-groupe de G contenant  $A \cup B$ , ie le groupe engendré par  $A \cup B$ .

$S \neq \emptyset$ , si  $x = x_1 \dots x_{2n+1}$  et  $y = y_1 \dots y_{2m+1}$  sont dans S,  $xy$  l'est aussi. Enfin,

$$(x_1 x_2 \dots x_{2n+1})^{-1} = x_{2n+1}^{-1} \dots x_2^{-1} x_1^{-1} \quad \text{et} \quad x_{2i}^{-1} \in A, x_{2i+1}^{-1} \in B \quad \text{donc } x^{-1} \in S.$$

S est bien un sous-groupe.

b) Si  $AB = BA$ , les éléments  $x_1 x_2 \dots x_{2n+1}$  de S s'écriront, après permutation, dans AB. Inversement, si  $ab \in AB$ , clairement  $a \in S$ . Donc  $S = AB$ .

$$\text{Si } S = AB, \text{ et si } a \in A \text{ et } b \in B, \text{ eba} \in S = AB \Rightarrow \boxed{BACAB}$$

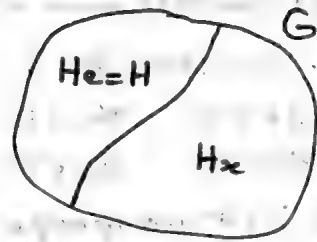
Cette inclusion entraîne que  $AB \subset BA$  puisque :

$$\forall a \in A \quad \forall b \in B \quad b^{-1}a^{-1} \in BACAB \Rightarrow \exists a' \in A \quad \exists b' \in B \quad b^{-1}a^{-1} = a'b' \Rightarrow ab = b'^{-1}a'^{-1} \in BA$$

(NB: Autre approche au VRamien ex Algèbre n° 2.1.18, et prolongements)



③ Soit  $H$  un sous-groupe d'indice 2 de  $G$ .



$$G = He \cup Hx$$

On doit prouver que :

$$\forall g \in G \quad \forall h \in H \quad \exists h' \in H \quad ghg^{-1} = h'$$

Par l'absurde : Si  $\exists g \in G \exists h \in H \quad ghg^{-1} \notin H$ , alors  $ghg^{-1} \in Hx$  et il existe  $h' \in H$  tel que  $ghg^{-1} = h'x$

De 2 choses l'une : \* ou bien  $hg^{-1} \in H \Rightarrow g^{-1} \in H \Rightarrow x = h^{-1}ghg^{-1} \in H$  absurde  
 \* ou bien  $hg^{-1} \in Hx \Rightarrow \exists h_1 \in H \quad hg^{-1} = h_1x$  d'où  $gh_1x = h'x$   
 puis  $gh_1 = h' \Rightarrow g = h'h_1^{-1} \in H$  ce qui est absurde car on retombe dans le 1<sup>er</sup> cas.

$H$  sera donc distingué dans  $G$ .

↓ 1<sup>re</sup> solution : Le raisonnement direct fonctionne.

Montrons que  $\forall g \in G \quad \forall h \in H \quad ghg^{-1} \in H$

De 2 choses l'une : si  $g \in H$ , c'est évident.

$$\text{si } g \in Hx, \quad g = h'x \quad \text{et} \quad ghg^{-1} = \underbrace{h'x}_{xh} h x^{-1} h'^{-1}$$

$xh \notin H$  (sinon  $x \in H$ )

$$\text{donc } xh \in Hx \Rightarrow xh = h''x$$

$$\text{Alors } ghg^{-1} = h' \underbrace{h''x}_{e} x^{-1} h'^{-1} \in H \quad \text{QED}$$

2<sup>e</sup> solution : La plus subtile :

Les classes à droites  $Hx$  et les classes à gauche  $xH$  forment une partition de  $G$ , en 2 parties seulement, par hypothèse. Comme l'une de ces 2 parties est  $H = He = eH$ ,

on conclut évidemment :  $Hx = xH$  ie  $H \triangleleft G$ . QED

Soient  $G$  un groupe et  $H$  un sous-groupe distingué de  $G$ .

1)  $Mq$   $T$  est un sous-groupe distingué de  $G/H$  si il est de la forme  $K/H$  où  $H \subset K \triangleleft G$ .

En déduire une bijection de l'ensemble des sous-groupes distingués de  $G$  contenant  $H$  sur l'ensemble des sous-groupes distingués de  $G/H$ .

2) Si  $H \subset K \triangleleft G$ ,  $mq$  :  $\frac{G/H}{K/H} \cong \frac{G}{K}$

3) Application : Quels sont les sous-groupes de  $\mathbb{Z}/n\mathbb{Z}$ ? Exhiber tous les sous-groupes de  $\mathbb{Z}/12\mathbb{Z}$ .

4)  $Mq$   $H$  est un sous-groupe distingué maximal de  $G$  si  $G/H$  est simple (ie ne possède pas de sous-groupes distingués non triviaux)

1) Soit  $\pi: G \rightarrow G/H$  la proj. can. Si  $T$  est un sous-groupe distingué de  $G/H$ ,  $\pi^{-1}(T)$  sera un sous-groupe distingué de  $G$  (comme l'image réciproque d'un sous-groupe distingué par un morphisme de groupe), il contient  $H$  et  $\pi(\pi^{-1}(T)) = T$  (car  $\pi$  surjective). Si l'on pose  $K = \pi^{-1}(T)$ , on aura :

$$H \subset K \triangleleft G \quad \text{et} \quad T = \pi(K) = K/H$$

Réc., si  $T = \pi(K)$  où  $H \subset K \triangleleft G$ , alors  $\pi(K) \triangleleft G/H$  (c'est un résultat général : si  $\beta: G \rightarrow G'$  est un morphisme de groupes et si  $K \triangleleft G$ , alors  $\beta(K) \triangleleft \beta(G)$ . Ici  $\pi$  est surjective).

\* Notons :  $\mathcal{G}$  = ens. des sous-groupes distingués de  $G$  contenant  $H$   
 $\mathcal{Q}$  = ens. des sous-groupes distingués de  $G/H$

L'application  $\Psi: \mathcal{G} \rightarrow \mathcal{Q}$  est une bijection  
 $K \mapsto \pi(K) = K/H$

On vient de montrer qu'elle est surjective. Montrons son injectivité. Elle découle du résultat suivant :

$$\forall K \in \mathcal{G} \quad \pi^{-1}(\pi(K)) = K \quad (*)$$

On a tjrs  $\pi^{-1}(\pi(K)) \supset K$ , mais ici  $\pi$  n'est pas injective et on ne peut pas conclure rapidement à l'égalité. Mais :

$x \in \pi^{-1}(\pi(K)) \Rightarrow \pi(x) = \pi(k) \quad k \in K \Rightarrow \pi(xk^{-1}) = e \Rightarrow xk^{-1} \in H \Rightarrow x \in kH \subset K$  (car  $H \subset K$ ). D'où (\*) et l'injectivité.

2) 
$$\begin{array}{ccc} G/H & \xrightarrow{\varphi} & G/K \\ \bar{x} & \longmapsto & \bar{x} \end{array}$$
 est bien définie car  $x=y \Rightarrow xy^{-1} \in H \subset K \Rightarrow \bar{x}=\bar{y}$ .

$\varphi$  est un morphisme de groupes surjectif et  $\ker \varphi = \{x \in G/H \mid x \in K\} = K/H = \pi(K)$ .  
Par décomposition canonique :

$$\begin{array}{ccc} G/H & \xrightarrow{\varphi} & G/K \\ \downarrow & \nearrow \sim & \\ G/H / K/H & & \end{array}$$

d'où l'isomorphisme annoncé.

3) Les sous-groupes de  $\mathbb{Z}$  sont les  $p\mathbb{Z}$ , et  $n\mathbb{Z} \subset p\mathbb{Z} \Leftrightarrow p \mid n$ . Les sous-groupes de  $\mathbb{Z}/n\mathbb{Z}$  seront les  $p\mathbb{Z}/n\mathbb{Z}$  où  $p \mid n$ . Si  $n=pq$ , on vérifie :  $p\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z}$ .

Pour  $n=12$ ,  $\mathcal{D}_{12} = \{1, 2, 3, 4, 6, 12\}$  d'où les 6 sous-groupes :

$$\mathbb{Z}/12\mathbb{Z} ; \quad 2\mathbb{Z}/12\mathbb{Z} = \{0, 2, 4, 6, 8, 10\} \simeq \mathbb{Z}/6\mathbb{Z} ; \quad 3\mathbb{Z}/12\mathbb{Z} = \{0, 3, 6, 9\} \simeq \mathbb{Z}/4\mathbb{Z}$$

$$4\mathbb{Z}/12\mathbb{Z} = \{0, 4, 8\} \simeq \mathbb{Z}/3\mathbb{Z} ; \quad 6\mathbb{Z}/12\mathbb{Z} \simeq \{0, 6\} \simeq \mathbb{Z}/2\mathbb{Z} \quad \text{et} \quad 12\mathbb{Z}/12\mathbb{Z} \simeq \{0\}$$

4) Dire que  $H$  est un sous-groupe distingué maximal de  $G$  signifie que :

$$H \subset K \triangleleft G \Rightarrow K=H \text{ ou } G \quad (*)$$

Il suffit alors d'utiliser la bijection  $\varphi$  du 1) pour constater :

$$(*) \Leftrightarrow \mathcal{Q} = \{\varphi(H); \varphi(G)\} = \{\{e\}, G/H\} \Leftrightarrow G/H \text{ simple}$$

NB : la preuve directe, qui revient à redémontrer que  $\varphi$  est une bijection, est faite en  $\boxed{\text{T}}$ .

Soient  $N$  et  $M$  deux sous-groupes normaux (ie distingués) d'un groupe  $G$  tels que  $N \subset M$ . Démontrer que :

$$G/N / M/N \cong G/M$$

$$G/N = \{ \bar{x} / x \in G \} \quad \text{où } \bar{x} = y \Leftrightarrow xy^{-1} \in N$$

$$M/N = \{ \bar{x} / x \in M \} \quad (M/N \text{ a une existence indépendante de } G/N, \text{ mais est isomorphe à une partie de } G/N \text{ à savoir } \{ \bar{x} \in G/N / x \in M \}^{(*)})$$

$$G \longrightarrow G/N / M/N$$

$$x \longmapsto \bar{\bar{x}}$$

$$\bar{\bar{x}} = \text{classe de } \bar{x} \in G/N \text{ modulo } M/N$$

$$\bar{x} = \text{" de } x \in G \text{ modulo } N$$

- $\varphi$  est bien définie
- $\varphi$  est surjective comme composée de 2 surjections ( $x \mapsto \bar{x}$  et  $\bar{x} \mapsto \bar{\bar{x}}$ )
- $\varphi$  est un morphisme (comme composée de 2 morphismes de groupes)
- $x \in \text{Ker } \varphi \Leftrightarrow \bar{\bar{x}} = \bar{e} \Leftrightarrow \bar{x} \in M/N \Leftrightarrow x \in M$ , donc  $\text{Ker } \varphi = M$ .

Par décomposition canonique de  $\varphi$ , on constate :

$$G/M \cong G/N / M/N$$

[(\*)] Une autre façon de le comprendre est d'écrire :

$$G/N = \{ xN / x \in G \}$$

$$M/N = \{ xN / x \in M \}, \text{ de constater que } M/N \subset G/N \text{ et que } xN \subset M \subset G \text{ car } N \triangleleft M$$

Soit  $G$  un groupe à 6 éléments.

a) Montrer que  $G$  possède un élément  $a$  d'ordre 2 et un élément  $b$  d'ordre 3.

b) Montrer que l'on a  $ba = ab$  ou  $ba = ab^2$ .

En déduire que  $G \cong \mathbb{Z}/6\mathbb{Z}$  ou  $G \cong \mathcal{I}_3$ .

a)

\* S'il existe un élément  $x$  de  $G$  d'ordre 6, alors  $G \cong \mathbb{Z}/6\mathbb{Z} = \{0, 1, \dots, 5\}$  contiendrait 3 d'ordre 2 et 2 d'ordre 3.

\* Supposons maintenant qu'aucun él. de  $G$  n'est d'ordre 6.

Tout élément  $x$  de  $G \setminus \{e\}$  sera d'ordre 2 ou 3 (Lagrange).

• Si tous les él. de  $G$  sont d'ordre 2,  $x^2 = e \quad \forall x \in G$  entraîne que  $G$  est commutatif (car  $(ab)^2 = e \Rightarrow abab = e \Rightarrow ba = ab$ )

Si  $a \neq b$  sont distincts de  $e$ ,  $\{e, a, b, ab\}$  sera un sous-groupe d'ordre 4 de  $G$  ce qui est absurde puisque 4 ne divise pas 6.

• Si tous les él. sont d'ordre 3,  $G = \{e, a, a^2, b, b^2, c\}$

où  $\langle a \rangle = \{e, a, a^2\}$  et  $\langle b \rangle = \{e, b, b^2\}$ , et il n'y a plus de place pour le sous-groupe  $\langle c \rangle$  engendré par  $c$  (2 sous-groupes distincts de  $G$  d'ordre 3 ne peuvent s'intersecter hors de  $e$ , car si  $H$  et  $H'$  sont de tels sous-groupes,  $H \cap H'$  sera un sous-groupe de  $H$  donc d'ordre 1 ou 3 d'où  $H \cap H' = \{e\}$  ou  $H$ ).

Si  $H \cap H' = H$ ,  $H \subset H' \Rightarrow H = H'$  absurde)

Concl. Il existe un élément  $a$  d'ordre 2 et un élément  $b$  d'ordre 3 dans  $G$ .



b) Ainsi  $G = \{e, a, b, b^2, c, d\}$

avec  $\langle a \rangle = \{e, a\}$

$\langle b \rangle = \{e, b, b^2\}$

qui ne s'intersectent  
qu'en  $\{e\}$  (car  
d'ordres 2 et 3...)

$\left. \begin{array}{l} ab \notin \langle a \rangle \text{ (sinon } b \in \langle a \rangle) \\ \notin \langle b \rangle \text{ (sinon } a \in \langle b \rangle) \end{array} \right\} \Rightarrow \boxed{ab = c} \text{ par exemple}$

Dem.

$\left. \begin{array}{l} ab^2 \notin \langle a \rangle \\ \notin \langle b \rangle \end{array} \right\} \Rightarrow ab^2 \in \{c, d\} \text{ mais } ab^2 = c = ab \Rightarrow b = e \text{ absurde.}$

Donc  $\boxed{ab^2 = d}$

$\left. \begin{array}{l} ba \notin \langle a \rangle \\ \notin \langle b \rangle \end{array} \right\} \Rightarrow ba \in \{c, d\} \text{ d'où 2 cas possibles :}$

$\boxed{\begin{array}{l} ba = ab \\ \text{ou} \\ ba = ab^2 \end{array}}$

1<sup>er</sup> cas : Si  $ba = ab$ ,  $G = \{e, a, b, b^2, \overset{c}{ab}, \overset{d}{ab^2}\}$  sera commutatif, donc :

$(ab)^2 = b^2$

$(ab)^3 = ab \cdot b^2 = a$

$(ab)^4 = ab \cdot a = b$

$(ab)^5 = ab \cdot b = ab^2$

$(ab)^6 = ab \cdot ab^2 = e \text{ et } ab \text{ sera d'ordre 6, donc } G \cong \mathbb{Z}/6\mathbb{Z}$

2<sup>e</sup> cas : Si  $ba = ab^2$ , on construit la table de  $G$  en utilisant cette "pseudo-commutativité" et on constate l'isomorphisme entre  $G$  et  $\mathcal{F}_3$  :

\* cet  $d$  seront d'ordre 2 cas :

$c^2 = (ab)^4 = ab \cdot \underbrace{ab}_{ab^2} = a^2 b^3 = a^2 = e$

$d^2 = (ab^2)^2 = ab^2 ab^2 = ab \cdot \underbrace{ba}_{ab^2} \cdot b^2 = abab = (ab)^4 = c^2 = e$

					$ab$ c	$ab^2$ d
$\nearrow$	e	a	b	$b^2$		
e	e	a	b	$b^2$	c	d
a	a	e	c	d	b	$b^2$
b	b	d	$b^2$	e	a	c
$b^2$	$b^2$		e	b		
c	c				e	
d	d					e

Toute la table se complète alors en utilisant le fait que chaque ligne (resp. colonne) ne contient que des éléments distincts  $\neq e$ , ou en utilisant la pseudo-commutativité de  $a$  et  $b$  :  $ba = ab^2$ , ce qui ramène tout calcul d'un produit à une expression du style  $a^\alpha b^\beta$  où  $\alpha = 0$  ou  $1$   $\beta = 0$  ou  $1$  ou  $2$ .

\* d'identification à  $\mathcal{F}_3$  est la suivante (par ex.) :

$e = Id$

$a = (1, 2)$

$b = (1, 2, 3)$

$b^2 = (1, 3, 2)$

$c = ab = (1, 2) \cdot (1, 2, 3) = (2, 3)$

$d = ab^2 = (1, 2) \cdot (1, 3, 2) = (1, 3)$

On vérifie encore que  $ba = ab^2$  ie  $(1, 2, 3)(1, 2) = (1, 2)(1, 3, 2)$ , d'où une construction de la table de  $(\mathcal{F}_3, \circ)$  en tous points similaire ! . QED

## Groupes symétriques

$\mathcal{P}(E)$  = ensemble des permutations (ou substitutions) de  $E$

$(\mathcal{P}(E), \circ)$  est un groupe appelé groupe symétrique de  $E$

$\mathcal{P}(\mathbb{N}_n) \doteq \mathcal{P}_n$  est le groupe symétrique d'ordre  $n$ .

$$\# \mathcal{P}_n = n!$$

Dans toute la suite,  $\#E = n$ .

ex:  $\mathcal{P}_3$  a 6 éléments

$$\begin{aligned} \text{Id} \quad \tau_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1, 2) \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1, 2) \quad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\ \sigma_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3) \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1, 3, 2) \end{aligned}$$

$\tau_i$  = transpositions

$\sigma_i$  = cycles de longueur 3

ex: Dresser la table de  $\mathcal{P}_3$ . Constatons qu'il n'est pas abélien.

### I Orbite d'un élément, transpositions, cycles

$s \in \mathcal{P}(E)$  fixé.

$x \sim y \Leftrightarrow \exists k \in \mathbb{Z} \quad y = s^k(x)$  définit une relation d'équivalence.

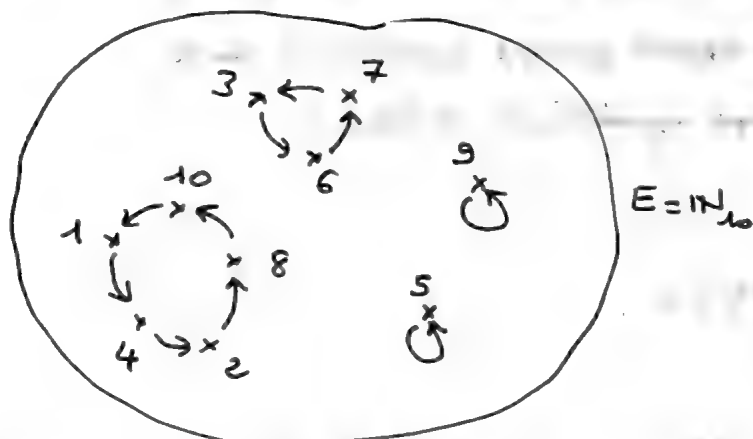
La classe d'~ de  $a$  s'appelle l'orbite de  $a$  suivant  $s$ . On note  $O_s(a)$ .

Un cycle est une permutation  $s$  qui ne possède qu'une et une seule orbite non réduite à 1 élément. Le cardinal de cette orbite est la longueur du cycle. Un cycle de longueur 2 est une transposition.

Le support d'une permutation  $s$  est  $\text{Supp } s = \{x \in E / s(x) \neq x\}$ .

## 1° Etude d'un exemple

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 8 & 6 & 2 & 5 & 7 & 3 & 10 & 9 & 1 \end{pmatrix}$$



Orbites :  $\sigma_1 = \{1, 4, 2, 8, 10\}$   $\sigma_3 = \{5\}$   $\sigma_9 = \{9\}$   $\sigma_3 = \{3, 6, 7\}$

Décomposition en produit de cycles :

$$\sigma = (1, 4, 2, 8, 10) \circ (3, 6, 7)$$

Décomposition en produit de transpositions :

On remarque que  $(3, 6, 7) = (3, 6)(6, 7)$  d'où :

$$\sigma = (1, 4)(4, 2)(2, 8)(8, 10)(3, 6)(6, 7)$$

## 2° Cas général : Théorèmes de décomposition

Prop : Soit  $\sigma$  une orbite suivant  $\sigma$ .

1)  $\sigma(\sigma) = \sigma$

2)  $\# \sigma \neq 1 \Rightarrow \forall a \in \sigma \quad \sigma(a) \neq a$

3)  $\# \sigma = p \Rightarrow \sigma = \{a, \sigma(a), \dots, \sigma^{p-1}(a)\}$  et  $\sigma^p(a) = a$  pour tout  $a \in \sigma$ .

preuve : 1)  $\forall a \in \sigma \quad \sigma \ni \{\sigma^k(a) / k \in \mathbb{Z}\}$ . Or  $\sigma(\sigma^k(a)) = \sigma^{k+1}(a)$  on tire  $\sigma(\sigma) \subset \sigma$ .

Comme  $\sigma$  est injective et  $\sigma$  fini, on conclut  $\sigma(\sigma) = \sigma$ .

2) Si  $\sigma(a) = a$ ,  $\sigma^k(a) = a$  pour tout  $k \in \mathbb{Z}$  donc  $\# \sigma = 1$

3) Soit  $p = \inf \{k \in \mathbb{N}^* / \sigma^k(a) = a\}$

Par div. euclidienne,  $k = pq + r$ ,  $0 \leq r < p$  donc  $\delta^k(a) = \delta^p \delta^q(a) = \delta^r(a)$

et  $\mathcal{O} = \{\delta^n(a) \mid 0 \leq n < p\}$ .

Si  $0 \leq n < n' < p$ ,  $\delta^n(a) = \delta^{n'}(a) \Leftrightarrow \delta^{n'-n}(a) = a$  et de  $0 \leq n'-n < p$  on tire  $n = n'$ . Finalement :

$\mathcal{O} = \{a, \delta(a), \dots, \delta^{p-1}(a)\}$  est formé de  $p$  éléments distincts  $\forall a \in E$ .

CQFD

Prop : Soient  $\sigma_1, \dots, \sigma_k$  des cycles de supports  $S_i$  disjoints  $\forall i \neq j$

1) Les  $\sigma_i$  commutent  $\forall i, j$ , donc  $\delta = \prod \sigma_i = \sigma_1 \dots \sigma_k$  est bien défini.

2) 
$$\begin{cases} \delta|_{S_i} = \sigma_i \\ \delta|_{E \setminus \bigcup S_i} = \text{Id} \end{cases}$$

3) Les  $S_i$  sont les orbites suivantes non réduites à 1 élément.

preuve :

1)  $\sigma_i \circ \sigma_j(x) = \begin{cases} \sigma_i(x) & \text{si } x \in S_i \\ \sigma_j(x) & \text{si } x \in S_j \\ x & \text{sinon} \end{cases}$  tout comme  $\sigma_j \circ \sigma_i$ .

2)  $\forall x \in S_i$  :  $\delta(x) = \sigma_1 \dots \sigma_k(x) = \sigma_i(x)$  car  $\begin{cases} \sigma_j(x) = x & \forall x \in S_i \\ \sigma_j(\sigma_i(x)) = \sigma_i(x) & \forall x \in S_i \end{cases}$

$\forall x \in E \setminus \bigcup S_i$  :  $\delta(x) = x$

3)  $\forall a \in E$  :  $\mathcal{O}_\delta(a) = \{\delta^k(a) \mid k \in \mathbb{Z}\}$

Si  $a \in E \setminus \bigcup S_i$  :  $\delta^k(a) = a$  donc  $\mathcal{O}_\delta(a) = \{a\}$  est réduite à 1 élément.

Si  $a \in \bigcup S_i$ , par ex.  $a \in S_i$ , alors  $\delta(a) = \sigma_i(a)$  d'où

$\mathcal{O}_\delta(a) = \{\sigma_i^k(a) \mid k \in \mathbb{Z}\} = \mathcal{O}_{\sigma_i}(a) = S_i$

CQFD

### Th. Décomposition d'une permutation en produit de cycles

Toute permutation <sup>distincte de Id</sup> s'écrit de façon unique (à l'ordre près) comme produit commutatif de cycles de supports  $\geq 2$  à 2 disjoints.

preuve:  $s \in \mathcal{P}(E)$

$S_1, \dots, S_k =$  orbites de  $s$  non réduites à 1 él.

$\sigma_i \doteq$  cycles de support  $S_i$  coïncidant avec  $s$  sur  $S_i$  ie  $\tau_q \left\{ \begin{array}{l} \sigma_i|_{S_i} = s|_{S_i} \\ \sigma_i|_{E \setminus S_i} = \text{Id}_{E \setminus S_i} \end{array} \right.$

Les  $S_i$  étant disjoints  $\geq 2$ ,  $s' \doteq \sigma_1 \dots \sigma_k$  est bien définie (cf Prop. préc.)

et:

$$\forall x \in S_i \quad j \neq i \Rightarrow \sigma_j(x) = x \quad \text{d'où} \quad s'(x) = \sigma_i(x) = s(x)$$

$$\forall x \in E \setminus \bigcup S_i \quad \forall j \quad \sigma_j(x) = x \quad \text{d'où} \quad s'(x) = x = s(x)$$

Donc  $s' = s$  et  $\boxed{s = \sigma_1 \dots \sigma_k}$ . La décomposition existe.

Unicité à l'ordre près: Si  $\sigma_1 \dots \sigma_k = \sigma'_1 \dots \sigma'_{k'}$ , les orbites démontrent que  $\hat{m}$  donc  $k = k'$  et  $S_i = S'_i$  (cf. Prop. préc.).

$$\text{Si } x \in S_i = S'_j \quad \left\{ \begin{array}{l} \sigma_1 \dots \sigma_k(x) = \sigma_i(x) \\ \sigma'_1 \dots \sigma'_{k'}(x) = \sigma'_j(x) \end{array} \right. \quad \text{d'où} \quad \sigma_i = \sigma'_j.$$

CQFD

De  $(a_1, a_2, \dots, a_p) = (a_1, a_2)(a_2, a_3) \dots (a_{p-1}, a_p)$  on déduit:

### Th. Décomposition d'une permutation en produit de transpositions

Toute permutation  $s$  de  $\mathcal{P}(E)$  s'écrit comme produit de transpositions (si  $n \geq 2$ )

Résultat que l'on peut affiner:



Th:  $\mathcal{P}_n$  ( $n \geq 2$ ) est engendré par les transpositions  $(i, i+1)$  où  $1 \leq i < n$ .

preuve:  $1 \leq p < q \leq n$

$(p, q)$  = produit de transpositions du type  $(i, i+1)$  ?

Réurrence sur  $q-p$ :

\* Si  $q-p=1$ , c'est trivial.

\* Si  $q-p > 1$ ,  $(p, q) = (q-1, q)(p, q-1)(q-1, q)$  fait aboutir la récurrence.  
CQFD

### 3° Intérêt

Reprenons l'exemple du 1° et calculons  $\sigma^{1000}$ .

$$\sigma = \sigma_1 \sigma_2 \quad \text{où} \quad \begin{cases} \sigma_1 = (1, 4, 2, 8, 10) \\ \sigma_2 = (3, 6, 7) \end{cases} \quad \begin{array}{l} \text{est d'ordre 5.} \\ \text{est d'ordre 3.} \end{array}$$

et  $\sigma_1, \sigma_2$  commutent. D'où  $\sigma^{1000} = \sigma_1^{1000} \sigma_2^{1000} = \text{Id} \cdot \sigma_2^{3 \times 333 + 1} = \sigma_2$ .

## II Signature d'une permutation

La signature de  $\sigma \in \mathcal{P}(E)$  est  $\epsilon(\sigma) = (-1)^{n-m}$  où  $m$  est le nbre d'orbites suivant  $\sigma$ .

$$\epsilon(\text{Id}) = 1$$

$$\tau \text{ transposition} \Rightarrow \epsilon(\tau) = (-1)^{n-(n-1)} = -1$$

$$\sigma \text{ cycle de longueur } p \Rightarrow \epsilon(\sigma) = (-1)^{n-(n-p+1)} = (-1)^{p-1}$$

$$\sigma = \text{permutation du I. 1°} \Rightarrow \epsilon(\sigma) = (-1)^{10-4} = 1$$

$$\epsilon(\sigma) = \epsilon((1, 4, 2, 8, 10)) \epsilon((3, 6, 7)) = (-1)^{5-1} (-1)^{3-1} = (-1)^4 (-1)^2 = 1 \cdot 1 = 1$$

$$\epsilon(\sigma) = \epsilon((1, 4, 2, 8, 10)) \epsilon((3, 6, 7)) = (-1)^{5-1} (-1)^{3-1} = (-1)^4 (-1)^2 = 1 \cdot 1 = 1$$

$$\| \underline{Th} : \forall \Delta \in \mathcal{F}(E) \quad \forall \tau \text{ transposition} \quad E(\Delta \tau) = -E(\Delta)$$

preuve:

$$\tau = \tau_{ab}$$

$$\Delta' = \Delta \tau_{ab}$$

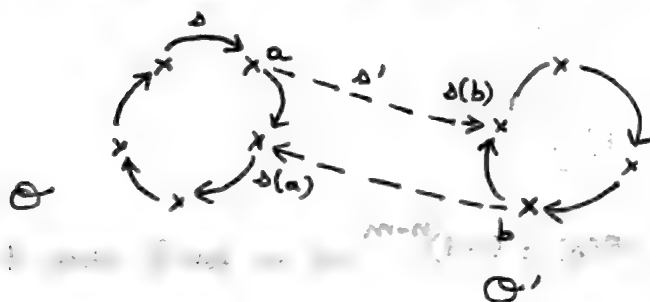
Seules les orbites suivantes contenant  $a$  ou  $b$  seront perturbées.

1-cas:  $a$  et  $b$  sont dans une même orbite  $\mathcal{O}$

$\mathcal{O}$  est partagée en 2 orbites suivantes :



2-cas:  $a \in \mathcal{O}, b \in \mathcal{O}'$  et  $\mathcal{O} \neq \mathcal{O}'$



Les 2 orbites  $\mathcal{O}$  et  $\mathcal{O}'$  sont recollées

Le nombre d'orbites change donc d'une unité quand on passe de  $s$  à  $s'$ .

CQFD

$$\| \underline{Co1} : \text{Si } \Delta = \tau_1 \dots \tau_R \text{ où } \tau_i \text{ transposition, } E(\Delta) = (-1)^R$$

$$\| \underline{Co2} : E : (\mathcal{F}(E), \circ) \longrightarrow (\{\pm 1\}, \times) \text{ est un morphisme surjectif de groupes.}$$

$$\Delta \longmapsto E(\Delta)$$

preuve: Décomposer  $\Delta$  en produit de transpositions puis utiliser le Co1 pour prouver  $E(\Delta \Delta') = E(\Delta) E(\Delta')$ . La surjectivité provient de  $E(\tau) = -1$  et  $E(\tau^2) = 1$ .

CQFD

Ainsi  $A_n \triangleq \text{Ker } E = \{s \in \mathcal{S}_n / E(s) = 1\}$  est un sous-groupe distingué de  $\mathcal{S}(E)$  appelé groupe alterné de degré  $n$ .

Par décomposition canonique de  $E$  :

$$\begin{array}{ccc} \mathcal{S}_n & \xrightarrow{E} & \{\pm 1\} \\ \downarrow & \nearrow \sim & \\ \mathcal{S}_n / A_n & & \end{array}$$

$s \in \mathcal{S}(E)$  est dite paire ou impaire suivant que  $E(s)$  vaille 1 ou -1. On constate qu'il y a autant de permutations paires que impaires en écrivant :

$$\begin{aligned} \# \mathcal{S} &= \underbrace{[\mathcal{S}_n : A_n]}_{\# \mathcal{S}_n / A_n} \cdot \# A_n \Rightarrow \# A_n = \frac{n!}{2} \\ &\doteq \# \mathcal{S}_n / A_n = 2 \end{aligned}$$

ex : prouver que  $\# A_n = \frac{n!}{2}$  directement (Sol. : utiliser la bij.  $A_n \rightarrow \mathcal{S}_n \setminus A_n$ )  
 $s \mapsto \tau s$

Soit  $\varphi$  un épimorphisme de groupes de  $G$  sur  $H$ . Soit  $T$  un sous-groupe de  $H$ .

a) Montrer que  $T \triangleleft H \Leftrightarrow \varphi^{-1}(T) \triangleleft G$

Dans cette hypothèse, prouver que  $G/\varphi^{-1}(T) \cong H/T$

b) Démontrer que  $\varphi$  induit une bijection des sous-groupes de  $G$  contenant  $\text{Ker } \varphi$  sur les sous-groupes de  $H$ . En déduire les sous-groupes de  $\mathbb{Z}/n\mathbb{Z}$ .

a) \*  $T \triangleleft H \Leftrightarrow \varphi^{-1}(T) \triangleleft G$  ?

$$(\Rightarrow) \quad \forall g \in G \quad \forall \varphi^{-1}(t) \in \varphi^{-1}(T) \quad g \varphi^{-1}(t) g^{-1} = \varphi^{-1}(\underbrace{\varphi(g) t \varphi(g)^{-1}}_{\in T}) \in \varphi^{-1}(T) \text{ oui}$$

(on n'a pas utilisé la surjectivité de  $\varphi$ )

Solution:  $\varphi^{-1}(T) = \text{Ker } \pi \circ \varphi$  où  $G \xrightarrow{\varphi} H \xrightarrow{\pi} H/T$ , donc  $\varphi^{-1}(T) \triangleleft G$ .

$$(\Leftarrow) \quad \forall h \in H \quad \forall t \in T \quad h t h^{-1} = \varphi(h_1 t_1 h_1^{-1}) \text{ où } h = \varphi(h_1) \\ t = \varphi(t_1) \Rightarrow t_1 \in \varphi^{-1}(T) \triangleleft G$$

Par hypothèse:  $h_1 t_1 h_1^{-1} \in \varphi^{-1}(T) \Rightarrow h t h^{-1} = \varphi(h_1 t_1 h_1^{-1}) \in T$  CQFD

(NB: Vérifier que si  $\varphi: G \rightarrow H$  est un morphisme de groupes, alors 1)  $T \triangleleft G \Rightarrow \varphi(T) \triangleleft \varphi(G)$  2)  $T \triangleleft H \Rightarrow \varphi^{-1}(T) \triangleleft G$ )

\* On obtient l'isomorphisme annoncé en décomposant canoniquement le morphisme de groupes:

$$\begin{array}{ccc} \tilde{\varphi} : G & \longrightarrow & H/T \\ x & \longmapsto & \varphi(x) \\ \downarrow & \nearrow & \\ G/\varphi^{-1}(T) & & \end{array}$$

$$\text{car } x \in \text{Ker } \tilde{\varphi} \Leftrightarrow \varphi(x) \in T \Leftrightarrow x \in \varphi^{-1}(T) \\ \text{ie } \text{Ker } \tilde{\varphi} = \varphi^{-1}(T)$$

b) Soient  $\mathcal{G}$  = ensemble des sous-groupes de  $G$  contenant  $\text{Ker } \varphi$

$\mathcal{H}$  = " " " de  $H$ .

$$\begin{array}{ccc} \hat{\varphi} : \mathcal{G} & \longrightarrow & \mathcal{H} \\ A & \longmapsto & \varphi(A) \end{array}$$

- L'image d'un sous-groupe par un morphisme de groupe est un sous-groupe, donc  $\hat{\varphi}$  est bien définie.

- Si  $T \in \mathcal{H}$ ,  $\varphi^{-1}(T)$  est un sous-groupe de  $G$  contenant  $\text{Ker } \varphi$  (car  $\varphi(n) = 0 \in T \Rightarrow n \in \varphi^{-1}(T)$ ) et  $\hat{\varphi}(\varphi^{-1}(T)) = \varphi\varphi^{-1}(T) = T$  (car  $\varphi$  surjective)  
Cela prouve que  $\hat{\varphi}$  est surjective.

-  $\hat{\varphi}$  est injective car  $\varphi(A) = \varphi(B) \Rightarrow \varphi^{-1}\varphi(A) = \varphi^{-1}\varphi(B) \Rightarrow A = B$   
 $A, B \in \mathcal{G}$  (lemme)

|| lemme : Si  $A \in \mathcal{G}$ , alors  $\varphi^{-1}\varphi(A) = A$

preuve : On a toujours  $A \subset \varphi^{-1}\varphi(A)$ . Réciproquement, si  $x \in \varphi^{-1}\varphi(A)$ ,  $\varphi(x) \in \varphi(A)$  soit  $\varphi(x) = \varphi(a)$  avec  $a \in A$ . D'où  $\varphi(xa^{-1}) = e \Rightarrow xa^{-1} \in \text{Ker } \varphi \subset A$   
 $\Rightarrow x \in Aa = A$  CQFD

\* Sous-groupes de  $\mathbb{Z}/n\mathbb{Z}$  :

Prendons  $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/n\mathbb{Z}$ . Les sous-groupes de  $\mathbb{Z}/n\mathbb{Z}$  seront les images des sous-groupes de  $\mathbb{Z}$  contenant  $\text{Ker } \varphi = n\mathbb{Z}$ , ie les  $\varphi(d\mathbb{Z})$  tels que  $d\mathbb{Z} \supset n\mathbb{Z}$ , ie les  $\varphi(d\mathbb{Z})$  avec  $d|n$ .

$$\text{NB : } \varphi(d\mathbb{Z}) = \{x \in \mathbb{Z}/n\mathbb{Z} / x \in d\mathbb{Z}\} \simeq d\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\frac{n}{d}\mathbb{Z}$$

Exemple : Sous-groupes de  $\mathbb{Z}/12\mathbb{Z}$

On a  $\text{Div}(12) = \{1, 2, 3, 4, 6, 12\}$ , d'où 6 sous-groupes de  $\mathbb{Z}/12\mathbb{Z}$ , à savoir :

$$\mathbb{Z}/12\mathbb{Z}$$

$$2\mathbb{Z}/12\mathbb{Z} = \{0, 2, 4, 6, 8, 10\} \simeq \mathbb{Z}/6\mathbb{Z}$$

$$3\mathbb{Z}/12\mathbb{Z} = \{0, 3, 6, 9\} \simeq \mathbb{Z}/4\mathbb{Z}$$

$$4\mathbb{Z}/12\mathbb{Z} = \{0, 4, 8\} \simeq \mathbb{Z}/3\mathbb{Z}$$

$$6\mathbb{Z}/12\mathbb{Z} = \{0, 6\} \simeq \mathbb{Z}/2\mathbb{Z}$$

$$12\mathbb{Z}/12\mathbb{Z} = \{0\}$$

LEMME D'ARTIN

Soient  $\Psi_1, \dots, \Psi_m$  des morphismes de groupe, tous distincts 2 à 2, d'un groupe  $G$  vers le groupe multiplicatif  $F^*$  d'un corps  $F$ . On se donne  $m$  éléments  $a_1, \dots, a_m$  de  $F$  non tous nuls en même temps.

Montrer qu'alors il existe au moins un élément  $g$  de  $G$  tel que :

$$a_1 \Psi_1(g) + \dots + a_m \Psi_m(g) \neq 0$$

(Ind. : raisonner par récurrence sur  $m$ )

\* Si  $m=1$ , c'est évident,  $a_1 \neq 0$  et  $\Psi_1(g) \in F^*$  entraînant  $a_1 \Psi_1(g) \neq 0$ .

\* Supposons la propriété vraie au rang  $m-1$ , et montrons qu'avec les hypothèses de l'énoncé :

$$\exists g \in G \quad a_1 \Psi_1(g) + \dots + a_m \Psi_m(g) \neq 0$$

Si l'un des  $a_i$  est nul, il suffit d'appliquer l'hypothèse récurrente et c'est vrai. Si tous les  $a_i$  ne sont pas nuls, supposons par l'absurde que :

$$\forall g \in G \quad a_1 \Psi_1(g) + \dots + a_m \Psi_m(g) = 0 \quad (1)$$

Pour tout  $h \in G$ , on aura :

$$a_1 \Psi_1(hg) + \dots + a_m \Psi_m(hg) = 0$$

$$a_1 \Psi_1(h) \Psi_1(g) + \dots + a_m \Psi_m(h) \Psi_m(g) = 0$$

$$a_1 \Psi_1(h) \Psi_m(h)^{-1} \Psi_1(g) + \dots + a_m \Psi_m(g) = 0 \quad (2)$$

En soustrayant (1) et (2), on obtient pour tout  $h$  et  $g$  dans  $G$  :

$$a_1 (1 - \Psi_1(h) \Psi_m(h)^{-1}) \Psi_1(g) + \dots + a_{m-1} (1 - \Psi_{m-1}(h) \Psi_m(h)^{-1}) \Psi_{m-1}(g) = 0$$

L'hypothèse récurrente montre que tous les coefficients des  $\Psi_i(g)$  doivent être nuls :



$$\forall i \in \mathbb{N}_{m-1} \quad a_i (1 - \Psi_i(h) \Psi_m(h)^{-1}) = 0$$

$$\text{d'où} \quad \forall h \in G \quad \Psi_m(h) = \Psi_i(h)$$

soit  $\Psi_m = \Psi_i$ , ce qui est contraire à l'hypothèse faite sur les  $\Psi_i$ .

CQFD

Montrer que 2 permutations conjuguées  $\sigma$  et  $\tau\sigma\tau^{-1}$  ont la même parité mais pas nécessairement le même nombre d'inversions (On pourra considérer  $\sigma = (1, 2, 3, 4)$  et  $\tau = (1, 4)$  dans  $\mathcal{I}_4$ )

$$* \quad E(\sigma) = E(\tau\sigma\tau^{-1}) \quad \text{car} \quad E(\tau\sigma\tau^{-1}) = E(\tau) \cdot E(\sigma) \cdot E(\tau) = E(\sigma)$$

$$* \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \text{a 3 inversions tandis que} \quad \tau\sigma\tau^{-1} = (4, 2, 3, 1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

en a 5.

Soit  $D$  un ensemble muni d'une loi interne associative ( $D$  est un demi-groupe)

Soit  $a \in D$ . On considère  $S = \{a, a^2, \dots, a^n, \dots\}$

a) Montrer que si  $S$  est fini, il existe 2 entiers  $m$  et  $n$  tels que  $m < n$  et  $a^m = a^n$ .

b)  $n$  étant choisi minimum dans la relation du a), on pose  $d = n - m$ .

Montrer que  $S = \{a, a^2, \dots, a^{n-1}\}$

c) Montrer que  $C = \{a^m, \dots, a^{n-1}\}$  est un groupe cyclique (isomorphe à  $\mathbb{Z}/d\mathbb{Z}$ ).

a) Si  $m \neq n \Rightarrow a^m \neq a^n$  alors  $S = \{a, a^2, \dots, a^n, \dots\}$  serait infini (car  $\varphi: \mathbb{N} \rightarrow S$  serait injective !)

$$n \mapsto a^n$$

b) Soit  $n = \inf \{p > m / a^m = a^p\}$ . Posons  $d = n - m \in \mathbb{N}^*$ .

$$a^k = a^{k-n} \cdot a^n = a^{k-n} \cdot a^m = a^{k-(n-m)} = a^{k-d} \quad \text{dès que } k \geq n$$

ou si l'on préfère :

$$\boxed{a^k = a^{k+d} = \dots = a^{k+vd} \quad \forall v \in \mathbb{N} \quad \forall k \geq m} \quad (*)$$

\* Si  $k \geq n$ , notons  $k = m + l$  et écrivons la div. euclidienne de  $l$  par  $d$  :

$$l = dq + r \quad 0 \leq r < d$$

$$\text{On a : } a^k = a^{m+dq+r} = a^{m+r} \quad \text{avec } m \leq m+r < m+d = n$$

$$\text{donc } \boxed{S = \{a, a^2, \dots, a^{n-1}\}}$$

c) D'après b), le produit de 2 éléments de  $C$  sera dans  $C$  ( $a^i \cdot a^j = a^k$ ).

Si  $m \leq k \leq n-1$ , on reste dans  $C$ . Sinon  $k \geq n$  et  $a^k = a^{m+r}$  avec  $m \leq m+r < n$  comme au b)).

Le produit est donc interne dans  $C$ .

\* Les él. de  $C$  sont distincts  $\Leftrightarrow a \neq b$  :

Si  $a^k = a^{k'}$ ,  $m \leq k < k' \leq n-1$ , alors  $a^{k+(n-k)} = a^{k'+(n-k)}$   
 $a^n = a^{n+(k'-k)}$   
 $a^{m+d} = a^{m+d+(k'-k)}$   
 $a^m = a^{m+(k'-k)}$  (cf (\*) dub)  
 absurde d'après la déf. de  $n$ , car  $0 < k'-k < n$

\* Soit  $\varphi: C \longrightarrow \mathbb{Z}/d\mathbb{Z}$   
 $a^k \longmapsto k$

$\varphi$  est surjective, injective (car chaque classe d'v  $k$  ne possède qu'un seul représentant  $k$  dans  $[m, n-1]$ , et vu que les él. de  $C$  sont distincts  $\Leftrightarrow a \neq b$ )  
 $\varphi$  est un morphisme car  $\varphi(a^k a^{k'}) = \varphi(a^{kk'}) = \overline{kk'} = \varphi(a^k) \varphi(a^{k'})$ , donc  
 $(C, \cdot)$  est un groupe par transport de structure.

NB : Un générateur de  $C$  sera  $a^{m+n}$  où  $m+n \equiv 1 \pmod{d}$ .

$$\{1, a, \dots, a^{d-1}\} = C$$

$H$  désigne un sous-groupe distingué d'un groupe  $G$ . On note  $\pi: G \rightarrow G/H$  l'épimorphisme canonique.

1)  $H \neq \pi$  induit une bijection croissante de l'ensemble des sous-groupes (resp. distingués) de  $G$  contenant  $H$  sur l'ensemble des sous-groupes (resp. distingués) de  $G/H$ .

2) On déduit que  $H$  est un sous-groupe distingué maximal de l'ensemble des sous-groupes distingués de  $G$  distincts de  $G$  (ie  $H \triangleleft G$  et  $H \subset K \triangleleft G \Rightarrow K=H$  ou  $G$ ) ssi  $G/H$  est simple (ie ne possède pas de sous-groupes distingués non triviaux).

(réf. résultat intéressant utilisé dans les suites de Jordan-Hölder : Quenée p16)

1)  $\pi$  étant un morphisme de groupes, l'image directe et l'image réciproque d'un groupe par  $\pi$  sera un s-groupe. Il est de plus aisé de vérifier que :

$$* \text{ Si } K \triangleleft G, \text{ alors } \pi(K) \triangleleft \pi(G) = G/H$$

$$* \text{ Si } T \triangleleft G/H \text{ alors } \pi^{-1}(T) \triangleleft G$$

$$* \text{ Si } T \text{ est un sous-groupe de } G/H \text{ alors } e \in T \Rightarrow \pi^{-1}(e) = H \subset \pi^{-1}(T)$$

Posons :  $\mathcal{G}$  = ens. des sous-groupes de  $G$  contenant  $H$

$\mathcal{G}_d$  = " " distingués de  $G$  contenant  $H$

$\mathcal{H}$  = ens. des sous-groupes de  $G/H$

$\mathcal{H}_d$  = " " distingués de  $G/H$

On peut définir les applications :

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{\varphi} & \mathcal{H} \\ K & \longmapsto & \pi(K) \end{array}$$

$$\begin{array}{ccc} \mathcal{H} & \xrightarrow{\psi} & \mathcal{G} \\ T & \longmapsto & \pi^{-1}(T) \end{array}$$

$$\begin{array}{ccc} \mathcal{G}_d & \xrightarrow{\varphi_d} & \mathcal{H}_d \\ K & \longmapsto & \pi(K) \end{array}$$

$$\begin{array}{ccc} \mathcal{H}_d & \xrightarrow{\psi_d} & \mathcal{G}_d \\ T & \longmapsto & \pi^{-1}(T) \end{array}$$

qui sont croissantes (car  $K \subset K' \Rightarrow \pi(K) \subset \pi(K')$  et  $T \subset T' \Rightarrow \pi^{-1}(T) \subset \pi^{-1}(T')$ )

Vérifions que  $\varphi$  et  $\psi$  (resp.  $\varphi_d$  et  $\psi_d$ ) sont inverses l'une de l'autre :

\*  $\pi$  surjective entraîne  $\pi(\pi^{-1}(T)) = T$

\* Si  $K$  est un sous-groupe de  $G$ , on a toujours  $\pi^{-1}(\pi(K)) \supset K$ , mais pas l'égalité en général. L'inclusion inverse provient de l'hypothèse supplémentaire  $K \supset H$ , comme on le voit :

$$\forall x \in \pi^{-1}(\pi(K)) \quad \pi(x) = \pi(k) \quad \text{où } k \in K$$

$$\pi(xk^{-1}) = e$$

$$xk^{-1} \in H$$

$$x \in Hk \subset K \quad \text{car } H \subset K$$

par suite  $\pi^{-1}(\pi(K)) \subset K$  et  $\pi^{-1}(\pi(K)) = K$  pour tout  $K \in \mathcal{G}$  (resp.  $\mathcal{G}_d$ )

2) H sous-groupe distingué maximal de  $G \iff G/H$  simple

( $\Rightarrow$ ) Soit  $T \triangleleft G/H$ . Alors  $\pi^{-1}(T) \triangleleft G$  et  $H \subset \pi^{-1}(T) \subset G$  entraîne

$$\pi^{-1}(T) = H \text{ ou } G, \text{ d'où } T = \pi(\pi^{-1}(T)) = \underbrace{\pi(H)}_{\{e\}} \text{ ou } \underbrace{\pi(G)}_{G/H}$$

$G/H$  est simple.

( $\Leftarrow$ ) Soit  $K \triangleleft G$  tel que  $H \subset K \triangleleft G$ .  $\pi(K)$  est un sous-groupe distingué de  $G/H$  qui est simple, donc  $\pi(K) = \{e\}$  ou  $G/H$  et :

$$K = \pi^{-1}(\pi(K)) = \underbrace{\pi^{-1}(e)}_H \text{ ou } \underbrace{\pi^{-1}(G/H)}_G$$

CQFD

Soient  $G$  et  $H$  deux groupes cycliques. Montrer que  $G \times H$  est cyclique  
ssi  $\Delta(|G|, |H|) = 1$ .

1<sup>ère</sup> solution : lemme : Soient  $a \in G$  et  $b \in H$ .  $\omega(a, b) = \text{ppcm}(\omega(a), \omega(b))$ .

En effet :  $(a, b)^k = (e, e') \Leftrightarrow (a^k, b^k) = (e, e') \Leftrightarrow \begin{cases} a^k = e \\ b^k = e' \end{cases} \Leftrightarrow \begin{cases} \omega(a) \mid k \\ \omega(b) \mid k \end{cases} \Leftrightarrow \text{ppcm}(\omega(a), \omega(b)) \mid k$ .

Cela étant démontré, posons  $\#G = m$  et  $\#H = n$ .

\*  $G \times H$  cyclique  $\Rightarrow \exists (a, b) \in G \times H$   $\omega(a, b) = mn$ .  $(a, b)$  engendre  $G \times H$  donc  $a$  et  $b$  engendrent resp.  $G$  et  $H$ , ie sont d'ordre  $m$  et  $n$ . D'après le lemme :

$$\omega(a, b) = \text{ppcm}(m, n) = mn \quad \text{ie } m \wedge n = 1$$

\* Réc. : si  $\text{ppcm}(m, n) = mn$  et si  $G = \langle a \rangle$ ,  $H = \langle b \rangle$ , on aura :

$$\omega(a, b) = \text{ppcm}(m, n) = mn \quad \text{donc } (a, b) \text{ engendre } G \times H$$

CQFD

2<sup>ème</sup> solution : Un groupe cyclique (ie monogène fini) est un groupe isomorphe à  $\mathbb{Z}/n\mathbb{Z}$ .

On peut donc supposer que  $G = \mathbb{Z}/n\mathbb{Z}$ ,  $H = \mathbb{Z}/p\mathbb{Z}$  et tout revient à prouver que :

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \text{ cyclique} \Leftrightarrow n \wedge p = 1$$

$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  ayant  $np$  éléments, tout revient à montrer que :

$$\boxed{\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/np\mathbb{Z} \Leftrightarrow n \wedge p = 1}$$

$$(\Leftrightarrow) \text{ C'est le Th. Chinois. } \begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \\ x & \longmapsto & (x, x) \end{array}$$

est un morphisme de noyau  $\mu\mathbb{Z}$  où  $\mu = \text{ppcm}(n, p)$  (car  $\varphi(x) = 0 \Leftrightarrow x \in n\mathbb{Z} \cap p\mathbb{Z} = \mu\mathbb{Z}$ )  
Par décomposition canonique :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \\ \pi \downarrow & & \uparrow \\ \mathbb{Z}/\mu\mathbb{Z} & \xrightarrow{\sim} & \Delta \text{Im } \varphi \end{array}$$

Si  $n \wedge p = 1$ ,  $\mu = np$  et  $\mathbb{Z}/\mu\mathbb{Z}$  possèdera  $np$  éléments,  $\Delta \text{Im } \varphi$  aussi et l'inclusion

$$\underbrace{\Delta \text{Im } \varphi}_{np \text{ él}} \subset \underbrace{\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}}_{np \text{ él}} \text{ entraîne que } \varphi \text{ est surjective, soit } \mathbb{Z}/\mu\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$



( $\Rightarrow$ ) Soit  $n, p$  deux entiers premiers entre eux,  $n, p \geq 2$ .

Supposons par l'absurde que  $np \neq 1$ . Soit  $d$  un diviseur commun à  $n$  et  $p$  et distinct de 1 :

$$n = dn'$$

$$p = dp'$$

$$\forall u = (x, y) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \quad dn'p' \cdot u = (np'x, pn'y) = (0, 0)$$

$$\text{donc } \omega(u) \mid dn'p'$$

Comme  $dn'p' < np$ , on constate que "tout élément de  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/np\mathbb{Z}$  est d'ordre strictement inférieur à  $np$ ". C'est absurde car il engendre  $\mathbb{Z}/np\mathbb{Z}$ .

QED

$$1 = q/n \quad \text{car } q/n = 1 \quad \text{car } q/n = 1$$

$$\begin{array}{c} \xrightarrow{q/n} \\ (n, n) \end{array}$$

$$\begin{array}{c} \xrightarrow{q/n} \\ \uparrow \\ \text{car } q/n = 1 \end{array}$$

$$\frac{q/n}{q/n} = \frac{q/n}{q/n} \quad \text{car } q/n = 1$$

Un groupe abélien est dit simple s'il n'est pas réduit à son élément neutre et s'il ne possède aucun sous-groupe différent de  $\{0\}$  et  $G$ . Alors :

$G$  groupe cyclique d'ordre premier  $\Leftrightarrow G$  groupe abélien simple.

( $\Rightarrow$ ) Tout groupe cyclique est abélien.  $G$  est d'ordre  $p$  premier, donc  $G \neq \{0\}$ .

Enfin, si  $H$  est un sous-groupe de  $G$ ,  $\#H \mid \#G = p$  donc  $H = \{0\}$  ou  $G$ .

( $\Leftarrow$ ) Si  $x \in G \setminus \{0\}$ ,  $G$  étant simple, le sous-groupe engendré par  $x$ , noté  $\langle x \rangle$ , ne pourra être que  $G$ . Donc  $G = \langle x \rangle$  et  $G$  est monogène.

$G$  sera donc isomorphe à  $\mathbb{Z}$  ou à  $\mathbb{Z}/n\mathbb{Z}$ .

$G$  est fini : Sinon  $f: \mathbb{Z} \rightarrow G$  est un isomorphisme, et si  $p \in \mathbb{N}^* \setminus \{1\}$ ,  

$$m \mapsto mx$$

$f(p\mathbb{Z})$  sera un sous-groupe de  $G$ , ie  $\{0\}$  ou  $G$  lui-même. Ce qui est absurde (car  $f$  est un isomorphisme).

$G$  d'ordre premier : D'après ce qui précède,  $G \cong \mathbb{Z}/n\mathbb{Z}$ . Si  $n$  était non premier, il existerait un diviseur  $d \in \mathbb{N}$  de  $n$  distinct de 1 et  $n$ , et on aurait :

$$\frac{\hat{n}}{d} \in \mathbb{Z}/n\mathbb{Z} \quad \text{et} \quad \omega\left(\frac{\hat{n}}{d}\right) = d$$

de sorte que  $\langle \frac{\hat{n}}{d} \rangle$  soit un sous-groupe d'ordre  $d$ , non trivial dans  $\mathbb{Z}/n\mathbb{Z}$ .

CQFD

Montrer que toute permutation paire peut se mettre sous la forme de produit de cycles de longueur 3.

En déduire que le groupe alterné  $\mathcal{A}_n$  est engendré par les cycles  $(1, 2, k)$  où  $3 \leq k \leq n$  (on suppose bien entendu  $n \geq 3$  dans ces questions)

\* Toute permutation paire est le produit d'un nombre pair de transpositions, soit :

$$\sigma = \tau_1 \tau'_1 \dots \tau_k \tau'_k$$

et le produit de 2 transpositions s'exprime en fct de cycles de longueur 3 car :

$$\begin{cases} (i, j)(j, k) = (i, j, k) \\ \text{ou} \\ (i, j)(k, l) = (i, j)(j, k)^2(k, l) = (i, j, k)(j, k, l) \end{cases} \quad (\text{si } i, j, k, l \text{ distincts } \& \& 2)$$

d'où le premier point.

\* D'après ce qui précède, tout revient à montrer que tout cycle d'ordre 3 s'exprime en fonction des  $(1, 2, k)$  où  $3 \leq k \leq n$ .

Soit  $(i, j, k)$  avec  $i < \inf(j, k)$ .

• 1-cas : Si  $i=1$ , on peut supposer  $j \neq 2$ .

$$\text{Si } k=2, \quad (1, j, 2) = (1, 2, j)^{-1}$$

$$\text{Si } k \neq 2, \quad (1, j, k) = (1, 2, k)^{-1} (1, 2, j) (1, 2, k)$$

• 2-cas : Si  $i=2$ , on a  $(2, j, k) = (1, 2, j)(1, 2, k)(1, 2, j)^{-1}$

• 3-cas : Si  $i > 2$ , on a  $(i, j, k) = (i, j)(j, k)$

$$= (i, j)(1, j)^2(j, k)$$

$$= \underbrace{(i, j)(1, j)}_{(1, j, i)} \underbrace{(1, j)(j, k)}_{(1, j, k)}$$

$$= (1, j, i)(1, j, k) \text{ qui s'écrivent en}$$

fonction des  $(1, 2, k)$  d'après le 1-cas.

Cel : Tout él. de  $\mathcal{A}_n$  s'écrit comme produit de cycles  $(1, 2, k)$  ou  $(1, 2, k)^{-1}$ . Si  $\mathcal{G}$  désigne le sous-groupe engendré par les cycles  $(1, 2, k)$ ,  $3 \leq k \leq n$ , on a  $\mathcal{A}_n \subset \mathcal{G}$ .

Les cycles  $(1, 2, k)$  étant de signature 1, ils sont dans le groupe alterné  $\mathcal{A}_n$  (des permutations paires), et l'on déduit  $\mathcal{G} \subset \mathcal{A}_n$ . Finalement  $\mathcal{G} = \mathcal{A}_n$ .

CQFD

Soit  $G$  un groupe de centre  $Z$  ( $Z = \{x \in G / \forall y \in G \ x y = y x\}$ )

a) Soit  $g \in G$ . Montrer que l'application  $\gamma_g : G \rightarrow G$  est un automorphisme  

$$x \mapsto g x g^{-1}$$

de  $G$ .  $\gamma_g$  est appelé automorphisme intérieur de  $G$ .

b) Montrer que l'ensemble  $\text{Int}(G)$  des automorphismes intérieurs de  $G$  est un sous-groupe distingué du groupe  $\text{Aut}(G)$  des automorphismes de  $G$ .

c) Démontrer que  $\text{Int } G \simeq G/Z$ .

a)  $\gamma_g(x x') = g x x' g^{-1} = g x g^{-1} g x' g^{-1} = \gamma_g(x) \cdot \gamma_g(x')$  montre que  $\gamma_g$  est un homomorphisme de  $G$  dans  $G$ . Comme  $\gamma_g(x) = y \Leftrightarrow g x g^{-1} = y \Leftrightarrow x = g^{-1} y g$ , on constate que  $\gamma_g$  est bijectif, ie un automorphisme de  $G$ .

NB: On constate aussi que  $\gamma_g^{-1} = \gamma_{g^{-1}}$ .

b)  $\text{Int } G = \{ \gamma_g / g \in G \}$  est un sous-groupe de  $\text{Aut}(G)$  car :

\*  $\text{Id} = \gamma_e \in \text{Int } G$

\* Si  $\gamma_g \in \text{Int } G$ , alors  $\gamma_g^{-1} = \gamma_{g^{-1}} \in \text{Int } G$

\* Si  $\gamma_g$  et  $\gamma_{g'}$  sont dans  $\text{Int } G$  :

$$\gamma_g \circ \gamma_{g'}(x) = \gamma_g(g' x g'^{-1}) = g g' x g'^{-1} g^{-1} = g g' x (g g')^{-1} = \gamma_{g g'}(x)$$

$$\text{soit } \gamma_g \circ \gamma_{g'} = \gamma_{g g'} \in \text{Int } G$$

⊗ Cette dernière relation implique que

$$\begin{array}{ccc} (G, \cdot) & \xrightarrow{\varphi} & (\text{Int } G, \circ) \\ g & \longmapsto & \gamma_g \end{array}$$

est un homomorphisme de groupes, surjectif par construction.

$$\begin{aligned} \text{Ker } \varphi &= \{ g \in G / \forall x \in G \ \gamma_g(x) = x \} = Z \text{ sera donc un sous-groupe distingué} \\ &\text{ie } g x g^{-1} = x \\ &\text{ie } g x = x g \end{aligned}$$

La décomposition canonique de  $\varphi$  donne :  $G/Z \simeq \text{Int } G$  d'où c).

⊗  $\text{Int } G \triangleleft \text{Aut } G$  est facile à montrer :

$$\forall \varphi \in \text{Aut } G \ \forall g \in G \quad \varphi \gamma_g \varphi^{-1}(x) = \varphi(g \varphi^{-1}(x) g^{-1}) = \varphi(g) x \varphi(g)^{-1} = \gamma_{\varphi(g)}(x)$$

$$\text{done } \varphi \gamma_g \varphi^{-1} = \gamma_{\varphi(g)} \in \text{Int } G.$$

QED

a) Soit  $G$  un groupe de centre  $Z$  tel que  $G/Z$  soit cyclique, montrer que  $G$  est abélien

b) Montrer que si  $G$  est un groupe fini non abélien de centre  $Z$ , alors  $\#G \geq 4 \#Z$ .

a) Tout groupe cyclique (ie monogène fini) est isomorphe à  $\mathbb{Z}/n\mathbb{Z}$  (avec  $n \neq 0$ ) de sorte que  $G/Z = \{e, a, a^2, \dots, a^{n-1}\}$

Si  $x \in G$ , il existe  $k \in [0, n-1]$  tq  $x = a^k$   
 ie  $x = ca^k$  où  $c \in Z$

De même, si  $y \in G$ , il existe  $l \in [0, n-1]$  tq  $y = c'a^l$  où  $c' \in Z$ .  
 Or aua :

$$xy = ca^k \cdot c'a^l = cc'a^{k+l} = c'a^l \cdot ca^k = yx$$

(car  $c$  et  $c'$  commutent avec tous, et  $a^k \cdot a^l = a^l a^k = a^{l+k}$ )

$G$  sera commutatif

b) Si  $\#G < 4 \#Z$ , alors  $\#G/Z = \frac{\#G}{\#Z} < 4$  et  $G/Z$  sera cyclique (d'ordre 1, 2 ou 3). Le a) vient de montrer qu'alors  $G$  est abélien, ce qui est absurde !

Soit  $V$  la partie de  $\mathcal{S}_4$  définie par :

$$V = \{ \text{Id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) \}$$

a) Montrer que  $V$  est un sous-groupe de  $\mathcal{S}_4$  et que  $V \triangleleft \mathcal{S}_4$ .

b) Démontrer que  $\mathcal{S}_4/V \cong \mathcal{S}_3$  et  $\mathcal{A}_4/V \cong \mathbb{Z}/3\mathbb{Z}$

Les éléments de  $V$  distincts de  $\text{Id}$  s'écrivent

$$(i,j)(k,l) \quad \text{où} \quad \{i,j,k,l\} = \{1,2,3,4\}$$

Clairément  $V \subset \mathcal{S}_4$  et  $(i,j)(k,l) = (k,l)(i,j)$  car ces perm. sont de supports disjoints.

a) \*  $V$  est un sous-groupe :

•  $V \neq \emptyset$

• Tous les produits possibles d'éléments de  $V$  (distincts de  $\text{Id}$ ) sont obtenus en considérant :

$$(i,j)(k,l) \circ (i,k)(j,l) = \begin{pmatrix} i & j & k & l \\ l & k & j & i \end{pmatrix} = (i,l)(j,k) \in V$$

$$\text{et } (i,j)(k,l) \circ (i,j)(k,l) = \text{Id}$$

• Clairément  $[(i,j)(k,l)]^{-1} = (i,j)(k,l) \in V$

NB :  $V$  est commutatif car  $\forall s \in V \quad s^2 = \text{Id}$

\*  $V \triangleleft \mathcal{S}_4$  ?

Soient  $s \in \mathcal{S}_4$  et  $h = (i,j)(k,l) \in V$ . Il s'agit de prouver que  $shs^{-1} \in V$ .

Gn a :

$$shs^{-1} = s(i,j)(k,l)s^{-1} = \begin{pmatrix} s(i) & s(j) & s(k) & s(l) \\ s(j) & s(i) & s(l) & s(k) \end{pmatrix} = (s(i), s(j))(s(k), s(l)) \in V$$

b)

$$* \# \mathcal{A}_4/V = \frac{\# \mathcal{A}_4}{\# V} = \frac{12}{4} = 3 \quad \text{donc } \mathcal{A}_4/V \cong \mathbb{Z}/3\mathbb{Z}$$

$$* \# \mathcal{S}_4/V = \frac{\# \mathcal{S}_4}{\# V} = \frac{24}{4} = 6 \quad \text{donc } \mathcal{S}_4/V \text{ sera un groupe isomorphe à } \mathbb{Z}/6\mathbb{Z} \text{ ou à } \mathcal{S}_3 \text{ (II).}$$

Tout revient donc à prouver que  $\mathcal{S}_4/V$  n'est pas commutatif.

1<sup>re</sup> méthode :

$$\underbrace{(1,2,3)}_{\sigma} \underbrace{(2,4)}_{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1,2,4,3)$$

$$\underbrace{(2,4)}_{\sigma} \underbrace{(1,2,3)}_{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (1,4,2,3)$$

$$\sigma \neq \sigma \circ \sigma \quad \text{car } \sigma \circ (\sigma \circ \sigma)^{-1} = (1,2,4,3)(1,3,2,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & & \end{pmatrix} \notin V$$

2<sup>e</sup> méthode : Par l'absurde. Si  $\mathcal{S}_4/V \cong \mathbb{Z}/6\mathbb{Z}$ , il existe un élément  $s$  de  $\mathcal{S}_4/V$  d'ordre 6.

$$s^k = \text{Id} \Rightarrow s^k = \text{Id} \Leftrightarrow 6 \mid k$$

Si  $k$  est l'ordre de  $s$ , on aura  $k \mid 24$  (Lagrange) et comme  $6 \mid k$ , on aura :  $k = 6$  ou  $12$  ou  $24$ .

- $k=24$  est à exclure car  $\mathcal{S}_4$  n'est pas commutatif
- $k=12 \Rightarrow \exists \sigma \in \mathcal{S}_4$  d'ordre 6 (prendre  $\sigma = s^2$ )
- $k=6$

Dans tous les cas, il existe une permutation  $\sigma$  de  $\mathcal{S}_4$  d'ordre 6. C'est absurde car tout  $\sigma \in \mathcal{S}_4$  s'écrit comme produit de cycles de supports disjoints, et avec 4 éléments on ne peut former aucun cycle de longueur 6 et aucun produit de cycles disjoints de longueur 2 et 3. QED



Les 2 questions peuvent être traitées indépendamment :

a) prouver que  $\mathcal{I}_n$  est engendré par les transpositions  $(i, n)$  où  $1 \leq i \leq n-1$

b) Mq  $\mathcal{I}_n$  est engendré par les transpositions  $(i, i+1)$  où  $1 \leq i \leq n-1$ . En déduire que  $\mathcal{I}_n$  est aussi engendré par les cycles  $\gamma = (1, 2, \dots, n-1)$  et  $\tau = (n-1, n)$  (On pourra expliciter  $\gamma^i \tau \gamma^{-i} \dots$ )

Rappel : On sait que toute permutation  $\sigma$  de  $\mathcal{I}_n$  s'écrit comme produit de cycles disjoints.

Tout cycle s'écrivant comme produit de transpositions :

$$(a_1, a_2, \dots, a_k) = (a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k)$$

on en déduit que les transpositions engendrent  $\mathcal{I}_n$ .

a) provient alors de :

$$(i, j) = (i, n)(j, n)(i, n)$$

b) \* Il faut écrire  $(i, j)$  comme produit de transpositions du type  $(i, i+1)$   $1 \leq i \leq n-1$ .

On montre que c'est possible par récurrence sur  $j-i$  :

$H(k)$  : " Si  $1 \leq j-i \leq k$  alors  $(i, j)$  est un produit de transpositions du type  $(i, i+1)$  "

-  $H(1)$  est vraie

- Si  $H(k-1)$  est vraie, soit  $(i, j)$  avec  $j-i = k > 1$ .

$$(i, j) = (j, j-1)(i, j-1)(j, j-1)$$

montre que  $(i, j)$  s'écrit encore comme produit des  $(i, i+1)$ . QED

(NB : Une seconde démonstration est proposée en remarque à la fin de la solution)

$$\begin{aligned} * \quad \gamma &= (1, 2, \dots, n-1) \quad \text{donc} \quad \begin{cases} \gamma(k) = k+1 \\ \gamma^2(k) = k+2 \\ \vdots \\ \gamma^i(k) = k+i \end{cases} \quad \text{en posant } m=k \Leftrightarrow m \equiv k [n-1] \\ \tau &= (n-1, n) \quad \text{(pour avoir } \gamma(n-1) = n = 1) \end{aligned}$$

On aura  $\gamma^{-i}(k) = k-i$ .

Calculons  $\gamma^i \tau \gamma^{-i}(k) = \gamma^i \tau(k-i) = \tau(k-i) + i$

→ Si  $k-i \notin \{n-1, n\}$  ie  $k \notin \{n+i-1, n+i\}$ , alors  $\gamma^i \tau \gamma^{-i}(k) = k$

→ Si  $k = n+i-1$  on a :  $\gamma^i \tau \gamma^{-i}(k) = n+i$

→ Si  $k = n+i$  on a :  $\gamma^i \tau \gamma^{-i}(k) = n+i-1$

Finalement  $\gamma^i \tau \gamma^{-i} = (n+i-1, n+i) = (i, i+1)$  et ce qui précède permet de conclure.

QED

.../...

NB : On peut utiliser le a) pour prouver la 1<sup>re</sup> partie de la question b).

En effet :  $\mathcal{I}_n$  est engendré par  $(1,2), \dots, (n-2,n-1)$

Par récurrence sur n :  $\mathcal{I}_2$  est engendré par  $(1,2)$ . Si  $\mathcal{I}_{n-1}$  l'est par  $(1,2), \dots, (n-2,n-1)$  alors tout élément de  $\mathcal{I}_n$  s'écrit comme produit des  $(i,n)$   $1 \leq i \leq n-1$  et :

$$(i,n) = \underbrace{(i,n-1)}_{\text{s'exprime en fonction de } (1,2), \dots, (n-2,n-1)} (n,n-1) \underbrace{(i,n-1)}_{\text{par hypothèse récursive}} \quad (\text{si } i < n-1)$$

montre que  $(i,n)$  s'exprime en fonction de  $(1,2), \dots, (n,n-1)$

CQFD

$$(1,n)(2,n)\dots(n,n) = (1,2)\dots(n,n-1)$$

Soient  $(G, \cdot)$  un groupe et  $x$  un élément de  $G$ . Notons  $C_x$  l'ensemble des éléments de  $G$  qui commutent avec  $x$ .

a) Montrer que  $C_x$  est un sous-groupe de  $G$ .

b) On appelle "centre de  $G$ ", et l'on note  $Z(G)$ , l'ensemble des éléments qui commutent avec tous les éléments de  $G$ .

Montrer que  $Z(G)$  est un sous-groupe distingué de  $G$ .

c) Vérifier que  $x \in Z(G) \Leftrightarrow C_x = G$

a) Immédiat :  $* C_x \neq \emptyset$  car  $ex = xe \Rightarrow e \in C_x$

$$* \forall y \in C_x \quad yx = xy \Rightarrow xy^{-1} = y^{-1}x \Rightarrow y^{-1} \in C_x$$

$$* \forall y, z \in C_x \quad yzx = yxz = xy z \Rightarrow yz \in C_x$$

b) \* Clairement  $e \in Z(G)$ , donc  $Z(G) \neq \emptyset$ .

$$* \forall x \in Z(G) \quad \forall g \in G \quad xg = gx \Rightarrow gx^{-1} = x^{-1}g \Rightarrow x^{-1} \in Z(G)$$

$$* \forall x, y \in Z(G) \quad \forall g \in G \quad xy g = xgy = gxy \Rightarrow xy \in Z(G)$$

$Z(G)$  est donc bien un sous-groupe de  $G$ . Il est distingué (\*) puisque :

$$\forall g \in G \quad \forall x \in Z(G) \quad gxg^{-1} = gg^{-1}x = x \in Z(G).$$

c)  $(\Rightarrow)$  Si  $x$  commute avec tout él. de  $G$ , on aura bien  $C_x = G$ .

$(\Leftarrow)$  Réc.  $C_x = G$  signifie que  $\forall g \in G \quad gx = xg$  i.e.  $x \in Z(G)$ .

(\*) Solution :  $Z(G)$  est le noyau du morphisme de groupes

$$\begin{aligned} G &\longrightarrow \mathcal{F}(G) \\ x &\longmapsto \beta_x(\cdot) = x \cdot x^{-1} \end{aligned}$$

qui à tout él.  $x$  de  $G$  associe l'automorphisme intérieur  $\beta_x$ .

On déduit directement que  $Z(G) \triangleleft G$ .

Soient  $G$  un groupe,  $H$  un sous-groupe de  $G$ , et  $G/H$  l'ensemble des classes à gauche suivant  $H$ .

- a) Montrer que  $G$  opère sur  $G/H$  par translation à gauche.
- b) Montrer que pour tout  $x$  de  $G$ , le groupe d'isotropie de  $xH$  est  $xHx^{-1}$ .
- c) Vérifier que le noyau  $K$  de l'action de  $G$  sur  $G/H$  est le plus grand sous-groupe distingué de  $G$  contenu dans  $H$ .

On suppose dans la suite que  $G$  est fini et  $H$  d'indice  $p$  où  $p$  est le plus petit entier divisant l'ordre de  $G$ .

- d) Montrer que  $[H : K]$  divise  $p!$ .
- e) Montrer que si  $q > 1$  divise  $[H : K]$  alors  $q \geq p$ .

f) Montrer que  $H \triangleleft G$ .

)) *dur: augmenter le nombre de questions intermédiaires!*

-----  
Solution :

- a)  $G/H$  = ens. des classes à gauche, pour :  $xRy \Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH$   
 Il y a compatibilité de  $R$  et, à gauche.

$\ell: G \rightarrow \mathcal{P}(G/H)$   
 $g \mapsto \ell_g$  où  $\ell_g(x) = \overline{gx}$  est un homomorphisme de groupes car :

$$\forall x \in G/H \quad \ell(gg')(x) = \overline{gg'x} = \ell(g)(\overline{g'x}) = \ell(g) \circ \ell(g')(x)$$

entraîne  $\boxed{\ell(gg') = \ell(g) \circ \ell(g')}$

Donc  $G$  agit sur  $G/H$ .

- b) Le sous-groupe d'isotrope de  $\bar{x} = xH$  est :

$$G_{\bar{x}} = \{g \in G / \ell_g(\bar{x}) = \bar{gx} = \bar{x}\}$$

Donc  $g \in G_{\bar{x}} \Leftrightarrow \bar{x}^{-1}gx \in H \Leftrightarrow g \in xHx^{-1}$

et  $\boxed{G_{\bar{x}} = xHx^{-1}}$

c)

$$\ell_g = Id \Leftrightarrow \forall x \quad \overline{gx} = \bar{x} \Leftrightarrow \forall x \quad g \in G_{\bar{x}} \Leftrightarrow g \in \bigcap_{x \in G} xHx^{-1}$$

Donc  $\boxed{K = \text{Ker } \ell = \bigcap_{x \in G} xHx^{-1}}$

On vérifie ensuite que  $\text{Ker } \ell$  est le plus grand sous-groupe distingué inclus dans  $H$  :

•  $\text{Ker } \ell \subset H$  puisque si  $x = e$ ,  $xHx^{-1} = H$ .

•  $\text{Ker } \ell$  est distingué car,

$$\forall y \in G \quad y(\text{Ker } \ell)y^{-1} = y \left( \bigcap_{x \in G} xHx^{-1} \right) y^{-1} \subset \bigcap_{x \in G} (yxH(yx)^{-1})$$

$$\bigcap_{x' \in G} x'Hx'^{-1} = \text{Ker } \ell$$

• Si  $S \trianglelefteq G$  et  $SCH$  alors  $S \subset \text{Ker } t$  :

En effet :

$$SCH \Rightarrow S = s s^{-1} C s H s^{-1}$$

pour tout  $s \in G$ , donc  $S \subset \bigcap_{s \in G} (s H s^{-1}) = \text{Ker } t$ .  $\square$

d) Par décomposition canonique de  $t$  :

$$\begin{array}{ccc} G & \xrightarrow{t} & \mathcal{I}(G/H) \cong \mathcal{I}(N_{[G:H]}) = \mathcal{I}(N_p) \\ \downarrow & \nearrow i & \\ G/\text{Ker } t & & \end{array}$$

$G/\text{Ker } t = G/K$

$G/K$  apparaît comme isomorphe à un sous-groupe de  $\mathcal{I}(N_p)$ , donc

$$|G/K| = [G:K] \text{ divise } |\mathcal{I}(N_p)| = p!$$

Il suffit de rappeler que

$$[G:K] = [G:H] [H:K]$$

pour constater que

$$[H:K] \mid [G:K] \mid p!$$

e) Vu l'hypothèse sur  $p$ , on peut poser

$$n = p^{\alpha} p_1^{\alpha_1} \dots p_R^{\alpha_R} \text{ où } p < p_1 < \dots < p_R ; p, p_i \text{ premiers}$$

Si  $q$  est premier et divise  $[H:K]$ , alors :

$$q \mid [H:K] \mid |H| \mid |G| \Rightarrow q \mid n \Rightarrow q \in \{p, p_1, \dots, p_R\} \Rightarrow q \geq p$$

Si  $q > 1$  divise  $[H:K]$ , il possède au moins un diviseur premier  $q_0$  et on applique ce qui précède :

$$q_0 \mid [H:K] \Rightarrow q_0 \geq p \Rightarrow q \geq p.$$

b) Comme  $K$  est le plus grand sous-groupe distingué de  $G$  inclus dans  $H$ , montrer que  $H \triangleleft G$  revient à montrer que  $K = H$ , ie

$$\boxed{[H:K] = 1} \quad (*)$$

Pour montrer (\*), on raisonne par l'absurde. S'il existe  $q$  premier qui divise  $[H:K]$ , d) et e) donnent :

$$\left. \begin{array}{l} q \mid p! \\ q \geq p \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} \exists k \quad q \mid k \text{ et } k \leq p \\ \text{et} \\ q \geq p \end{array} \right. \Rightarrow q = p$$

Cela entraîne  $[H:K] = p^\beta$  avec  $1 \leq \beta \leq \alpha$ .

La question d) entraîne alors :  $p^\beta \mid p!$ . Si l'on suppose  $\beta > 1$ , alors  $p^{\beta-1} \mid (p-1)!$  entraîne

$$p^{\beta-1} \equiv \underbrace{(p-1)!}_{\text{Th. Wilson}} \equiv -1 \quad (p)$$

ce qui est absurde. Donc  $\beta = 1$  et :

$$\boxed{[H:K] = p}$$

On en déduit :

$$[G:K] = [G:H] \times [H:K] = p^2$$

D'où (cf exercice 9ème p 24, ex 24)  $G/K$  <sup>commutatif</sup> ~~cyclique~~ !

~~$G/K$~~



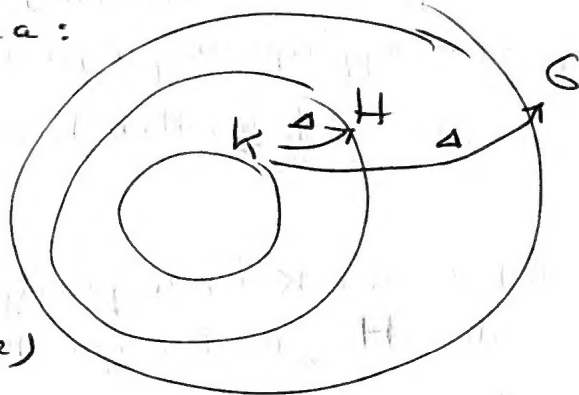
Il est alors facile de vérifier que  $H \trianglelefteq G$ , ce qui constitue l'absurdité puisqu'elle entraîne  $H = K$ . On a :

$$\forall h \in H \quad \forall x \in G \quad \overline{hxh^{-1}} = \overline{hx^{-1}h} = \overline{h} = h$$

Classes dans  $G/K$

car  $G/K$  commutatif

et  $K \trianglelefteq G$  (donc  $G/K$  est bien un gpe)



Donc :

$$\forall h \in H \quad \forall x \in G \quad h^{-1} \cdot (xhx^{-1}) \in K \subset H$$

$$\forall h \in H \quad \forall x \in G \quad xhx^{-1} \in hH = H$$

(et cela signifie bien que  $H \trianglelefteq G$ .)  $\square$